Encrypted information signal, information recording medium, information signal regenerating and recording device

Publication number: CN1313599
Publication date: 2001-09-19
Inventor: TAKAHIRO NAGAI (JP); HIDEYUKI NISHIHARA (JP); YOSHIHISA FUKUSHIMA (JP)
Applicant: MATSUSHITA ELECTRIC IND CO LTD (JP)
Classification:
- international: ***G11B20/00; H04N5/85;*** *G11B20/12; H04N1/00; H04N9/804;* **G11B20/00; H04N5/84;** G11B20/12; H04N1/00; H04N9/804; (IPC1-7): G11B20/10; G09C5/00; G11B23/30
- European: G11B20/00P; H04N5/85
Application number: CN20011009469 20010314
Priority number(s): JP20000070020 20000314

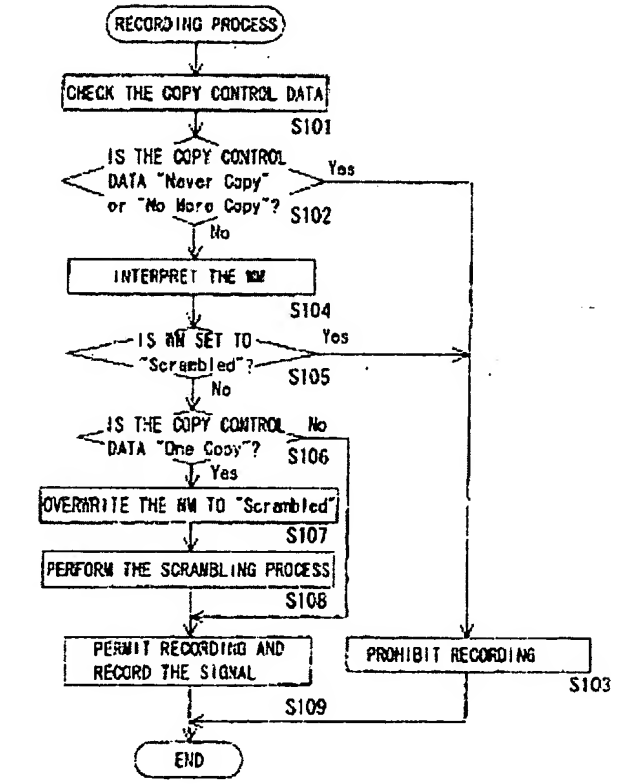
Also published as:
EP1134964 (A2)
US2002015494 (A1)
KR20010092320 (A)
EP1134964 (A3)
CN1165047C (C)

Report a data error here

Abstract not available for CN1313599
Abstract of corresponding document: **EP1134964**

Playing a data signal from an illegally produced data storage medium can be effectively disabled regardless of the type of storage medium so that copying can be prevented effectively at low cost. An encrypted data signal encrypting a copy-controlled data signal has superimposed thereto as a digital watermark identification data identifying the data signal as an encrypted signal. A data storage medium records this encrypted data signal, a data signal player reproduces the signal, and a data signal recorder records the signal.

Fig. 4



[19]中华人民共和国国家知识产权局

[51]Int. Cl[7]
G11B 20/10
G11B 23/30 G09C 5/00

[12]发明专利申请公开说明书

[21]申请号 01109469.9

[43]公开日 2001年9月19日

[11]公开号 CN 1313599A

[22]申请日 2001.3.14 [21]申请号 01109469.9

[30]优先权

[32]2000.3.14 [33]JP [31]70020/2000

[71]申请人 松下电器产业株式会社

地址 日本大阪府

[72]发明人 永井隆弘 石原秀志 福岛能久

[74]专利代理机构 中科专利商标代理有限责任公司

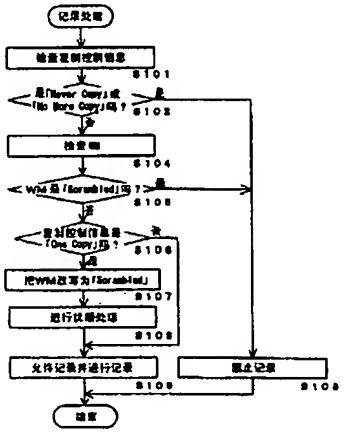
代理人 汪惠民

权利要求书4页 说明书25页 附图页数16页

[54]发明名称 加密信息信号、信息记录介质、信息信号再生及记录装置

[57]摘要

一种加密信息信号、记录了该信号的信息记录介质、再生该信号的 信息信号再生装置以及记录该信号的信息信号记录装置，该加密信息信 号是对作为复制控制对象的信息信号加密的加密信息信号，该信息信号 为识别处于被加密了的状态的信号的识别信息作为电子水印信息被叠加 的信号。不管记录介质的种类如何也可以使从非法复制成的记录介质进 行信息信号的再生实际上成为不可能，有效、低成本地防止非法复制。



ISSN1008-4274

权 利 要 求 书

1. 一种加密信息信号，是一种对作为复制控制对象的信息信号加密的加密信息信号，其特征在于是识别上述信息信号为处于被加密了的状态的信号的识别信息作为电子水印信息被叠加的信号。

2. 根据权利要求 1 所述的加密信息信号，其特征在于上述信息信号为至少被施以禁止除此以外的复制和绝对禁止复制中的一种限制的信息信号。

3. 根据权利要求 1 所述的加密信息信号，其特征在于上述电子水印信息还包含表示记录有上述加密信息信号的信息记录介质的类别的类别信息。

4. 一种信息记录介质记录有根据权利要求 1 所述的加密信息信号。

5. 根据权利要求 4 所述的信息记录介质，其特征在于是还记录有被加密了的第 1 锁和被加密了的第 2 锁的信息记录介质，上述第 1 锁为用于加密被电子水印信息叠加的上述信息信号的锁，上述第 2 锁为用于加密上述第 1 锁的锁。

6. 一种信息信号再生装置，其特征在于具备有从根据权利要求 4 所述的信息记录介质读出加密信息信号的读出部、判别读出部所读出的上述加密信息信号处于加密状态的加密状态判别部、解读上述加密信息信号并取出被电子水印信息叠加的信息信号的解读部、从解读部解读的上述信息信号抽出上述电子水印信息并判别表示上述识别信息的内容的电子水印信息解码部、比较由加密状态判别部所判别的状态和由电子水印信息解码部所判别的表示识别信息的状态且在不一致的情况下禁止上述信息信号的再生的再生控制部。

7. 根据权利要求 6 所述的信息信号再生装置，其特征在于加密状态判别部在解读部取出了信息信号的情况下判别上述加密信息信号处于被加密的状态。

8. 根据权利要求 6 所述的信息信号再生装置，其特征在于上述电子水印信息还包含有表示记录有上述加密信息信号的信息记录介质的类

别的类别信息，信息信号再生装置还具备有判别上述信息记录介质的类别的类别判别部，在由上述类别信息所表示的信息记录介质的类别和由类别判别部所判别的信息记录介质的类别一致的情况下，再生控制部允许上述信息信号的再生。

9. 根据权利要求 6 所述的信息信号再生装置，其特征在于在上述信息记录介质中还记录有被加密了的第 1 锁和被加密了的第 2 锁，上述第 1 锁为用于加密被电子水印信息叠加的上述信息信号的锁，上述第 2 锁为用于加密上述第 1 锁的锁，解读部用于加密上述第 2 锁，保持有固定分配给信息信号再生装置的第 3 锁，解读由上述第 3 锁加密的第 2 锁并取得上述第 2 锁，解读由取得的上述第 2 锁加密的第 1 锁并取得上述第 1 锁，解读由取得的上述第 1 锁加密的上述加密信息信号并取出被电子水印信息叠加的信息信号。

10. 根据权利要求 8 所述的信息信号再生装置，其特征在于信息信号再生装置是由包含读出部、加密状态判别部及类别判别部和第 1 认证部的驱动装置，包含解读部、电子水印信息解码部及再生控制部和第 2 认证部的解码装置和连接驱动装置和解码装置的接口构成；上述第 1 认证部和上述第 2 认证部通过上述接口进行通信，上述第 1 认证部认证解码装置是否为符合装置，上述第 2 认证部认证驱动装置是否为符合装置；在上述第 1 认证部和上述第 2 认证部之间认证成立的情况下，再生控制部允许信息信号的再生。

11. 根据权利要求 10 所述的信息信号再生装置，其特征在于在上述信息记录介质中还记录有用于上述第 1 认证部及上述第 2 认证部各自认证的第 1 认证锁及第 2 认证锁，第 1 认证部具有被固定分配给驱动装置的第 1 设备锁，根据上述第 1 认证锁、上述第 1 设备锁和类别判别部所判别的上述信息记录介质的类别生成第 1 介质认证锁，第 2 认证部具有被固定分配给解码装置的第 2 设备锁，根据上述第 2 认证锁和上述第 2 设备锁生成第 2 介质认证锁，上述第 1 认证部和上述第 2 认证部比较上述第 1 介质认证锁和上述第 2 介质认证锁并进行认证。

12. 根据权利要求 11 所述的信息信号再生装置，其特征在于第 2 认证部至少利用因信息记录介质而异的认证步骤及信息信号传输步骤中的

一方检测出信息记录介质的类别。

13. 一种信息信号记录装置，是一种把作为复制控制对象的信息信号记录在信息记录介质上的信息信号记录装置，其特征在于具备有把识别上述信息信号为处于被加密了的状态的信号的识别信息作为电子水印信息叠加到信息信号上的电子水印信息处理部、对通过上述电子水印信息处理部被上述电子水印信息叠加的信息信号加密并生成加密信息信号的加密部、把由加密部生成的加密信息信号写入信息记录介质的写入部。

14. 根据权利要求 13 所述的信息信号记录装置，其特征在于还具备有判别上述信息记录介质的类别的类别判别部，上述电子水印信息还包含表示由类别判别部的记录有上述加密信息信号的上述信息记录介质的类别的类别信息。

15. 根据权利要求 14 所述的信息信号记录装置，其特征在于还具备有抽出被叠加在信息信号上的电子水印信息并判别表示上述识别信息的内容的电子水印信息解码部、根据由电子水印信息解码部所判别的上述识别信息许可记录的记录控制部。

16. 根据权利要求 15 所述的信息信号记录装置，其特征在于信息信号记录装置是由包含写入部、类别判别部和第 1 认证部的驱动装置，包含加密部、电子水印信息处理部、电子水印信息解码部、记录控制部和第 2 认证部的编码装置和连接驱动装置和编码装置的接口构成；上述第 1 认证部和上述第 2 认证部通过上述接口进行通信，上述第 1 认证部认证编码装置是否为符合装置，上述第 2 认证部认证驱动装置是否为符合装置，在上述第 1 认证部和上述第 2 认证部之间认证成立的情况下，记录控制部允许上述信息信号的记录。

17. 根据权利要求 16 所述的信息信号记录装置，其特征在于在上述信息记录介质中还记录有用于上述第 1 认证部及上述第 2 认证部各自认证的第 1 认证锁及第 2 认证锁，第 1 认证部具有被固定分配给驱动装置的第 1 设备锁，根据上述第 1 认证锁、上述第 1 设备锁和类别判别部所判别的上述信息记录介质的类别生成第 1 介质认证锁，第 2 认证部具有被固定分配给编码装置的第 2 设备锁，根据上述第 2 认证锁和上述第 2 设备锁生成第 2 介质认证锁，上述第 1 认证部和上述第 2 认证部比较上

述第 1 介质认证锁和上述第 2 介质认证锁并进行认证。

18. 根据权利要求 17 所述的信息信号记录装置，其特征在于第 2 认证部至少利用因信息记录介质而异的认证步骤及信息信号传输步骤中的一方检测出信息记录介质的类别。

19. 根据权利要求 13 所述的信息信号再生装置，其特征在于在上述信息记录介质中记录有由被固定分配给信息信号再生装置的第 3 锁加密的第 2 锁；加密部在加密部内部产生随机数，根据被记录在上述信息记录介质上的第 1 锁信息或被叠加在电波上的第 1 锁信息取得上述第 1 锁，用第 1 锁加密被电子水印信息叠加的信息信号，用第 2 锁加密上述第 1 锁，根据第 3 锁和记录在信息记录介质上的加密了的第 2 锁取得第 2 锁。

20. 根据权利要求 19 所述的信息信号记录装置，其特征在于写入部还把由第 2 锁加密的第 1 锁写入信息记录介质。

说　　明　　书

加密信息信号、信息记录介质、信息信号再生及记录装置

本发明涉及一种在把数字化的作品如图像、音乐等信息信号记录在信息记录介质时限制非法复制的技术以及限制从被非法复制了的信息记录介质上再生的技术。

近年来，随着数字化内容的普及，对数字化内容的非法复制所引起的著作权侵权就成了大问题。为了防止非法复制，可以考虑把用于控制复制的信息（复制控制信息）加在数字化内容上的技术或使用加密技术对信息信号进行加密而使得在除正式被授权的机器之外的机器上无法进行解码（解读）的技术。此外，还存在把复制控制信息作为电子水印信息嵌在信息信号中的技术。电子水印信息被作为噪音叠加在信息信号上的，不容易被改写，因此，即便在复制控制信息被非法改写了的情况下也可以进行再生控制及记录控制。

为了控制复制而被加在信息信号上的信息有“可复制（Copy Free）”、“只能复制 1 次(One Copy)”、“禁止除此以外的复制（No More Copy）”、“绝对禁止复制(Never Copy)”这四种状态。根据这四种状态可以表现信息信号的复制世代和复制控制状态。

复制的限制依照如下进行。具体来说，记录装置检查包含在图像、音乐等信息信号中的复制控制信息，如果复制控制信息为“禁止除此以外的复制”或“绝对禁止复制”则对记录进行限制。由此实现复制世代限制。但是，不检查复制控制信息的记录装置可以把处于“禁止除此以外的复制”状态的信息信号记录在记录介质上，而且，与包含复制控制信息的原来的信息信号一样的信息信号依照原样被复制在此记录介质上，这样，著作权就得不到保护。

作为用于解决此问题的技术，在特开平 11-353796 公报中记载有这样的技术，即把电子水印信息叠加在信息信号上并在再生信息信号时改变

电子水印信息的表示状态，由此使得从被非法记录的记录介质进行的再生实际上成为不可能。

下面更具体地进行说明。在此说明中，把与电子水印信息的解读处理或写入处理对应的称为“符合”、不对应的称为“非符合”。图 16 为表示以往的复制控制的原理的图。在 DVD-RAM 等 RAM 盘 1300 中记录有重叠着表示“禁止除此以外的复制”的复制控制信息(CGMS[11])和同样表示“禁止除此以外的复制”的电子水印信息(WM[No More Copy])的信息信号。在再生此信息信号时，符合再生装置 1301 把电子水印信息从“No More Copy”（禁止除此以外的复制）改写为“Never Copy”(绝对禁止复制)并重新叠加在信息信号上，再把信息信号作为再生输出信号送出。通常，在 DVD-RAM 中，在禁止复制的情况下利用“No More Copy”而不利用“Never Copy”。因此，当检测出被叠加在信息信号上的电子水印信息为“Never Copy”时，符合记录装置 1302 就不记录该信息信号。由此可以控制复制。

另一方面，非符合记录装置 1303 不管电子水印信息的内容不受记录限制地把信息信号记录在别的 RAM 盘 1304 上。但是，被非法记录的 RAM 盘 1304 的电子水印信息为“Never Copy”。因此，符合再生装置 1305 通过读取该电子水印信息判断该 RAM 盘 1304 是进行过非法复制的记录介质，使再生实际上成为不可能。

如上所述，为了控制复制，以往的符合再生装置 1301 把电子水印信息的内容从“No More Copy”（禁止除此以外的复制）改写为“Never Copy”(绝对禁止复制)，因此，再生装置必须备有电子水印信息的改写部，造成再生装置的成本增加。

还有，上述的技术不能适用于 DVD-ROM。在 DVD-ROM 中，用于判定是否非法的电子水印信息“Never Copy”在通常的使用中要被写入存储盘的。

鉴于上述问题，本发明的目的在于不管记录介质的种类如何也可以通过使从非法复制成的记录介质进行信息信号的再生实际上成为不可能来有效、低成本地防止非法复制。

为了解决上述课题，基于本发明的复制世代管理，在记录控制复制所

必需的信息信号的信息记录介质中，其特征在于至少把表示以扰频状态被记录在信息记录介质上的扰频信息作为电子水印信息叠加在作为禁止除此以外的复制、绝对禁止复制的状态的上述信息信号上，是一种在被上述电子水印信息叠加的信息信号上实施扰频的信息信号。

本发明的信息记录再生装置是这样一种信息再生装置，把表示以扰频状态被记录在信息记录介质上的扰频信息作为电子水印信息叠加在作为禁止除此以外的复制或绝对禁止复制的状态的上述信息信号上，并读出记录有在被上述电子水印信息叠加的信息信号上实施扰频的信息信号的信息记录介质，具备有从信息记录介质读出信息的信息读出部、消去对上述信息信号进行的扰频的去扰频部、检测出作为电子水印信息叠加在被去扰频了的信息信号上扰频信息的电子水印信息检测部、考察上述电子水印信息和去扰频部的去扰频动作且至少在电子水印信息的扰频信息处于扰频状态且去扰频部不工作的情况下禁止上述信息信号的正常的再生的再生控制部。

本发明的信息记录装置是一种把具有可复制 1 次、禁止除此以外的复制或绝对禁止复制的状态的复制控制信息的上述信息信号写入信息记录介质的信息记录装置，具备有检测出上述复制控制信息的部、在检测出的复制控制信息为可复制 1 次的情况下把表示以扰频状态被记录在信息记录介质上的扰频信息作为电子水印信息叠加在上述信息信号上的电子水印信息改写部、在叠加了上述电子水印信息的信息信号上实施扰频的扰频部和把上述进行了扰频的信息信号写入信息记录介质的信息写入部。

本发明的信息信号记录装置，在把具有可复制 1 次、禁止除此以外的复制或绝对禁止复制的状态的复制控制信息的上述信息信号写入信息记录介质的信息记录装置中，具备有检测出上述复制控制信息的复制控制信息检测部、检测出被叠加在上述信息信号上的电子水印信息的电子水印信息检测部、在表示信息信号作为上述电子水印信息以扰频状态被记录的扰频信息被检测出的情况下禁止记录的记录控制部。

下面对附图进行简单说明。

图 1 为用于说明基于实施例 1 的复制世代管理方法的概略图。

图 2 为表示在对被扰频了的信号信息进行读出或写入时的数据的流程的图。

图 3 为表示符合记录装置的构成的图。

图 4 为表示记录装置的记录处理流程的流程图。

图 5 为表示符合再生装置的构成的图。

图 6 为表示再生处理流程的流程图。

图 7 为表示通过个人计算机（PC）记录系统实现符合记录装置的例子的图。

图 8 为表示在 PC 编码器的控制部上的处理流程的流程图。

图 9 为表示在 PC 记录驱动的控制部上的处理流程的流程图。

图 10 为表示通过个人计算机（PC）再生系统实现符合再生装置的例子的图。

图 11 为表示在 PC 驱动的控制部上的处理流程的流程图。

图 12 为表示 PC 解码器的控制部的处理流程的流程图。

图 13 为表示在传送存储盘类别的信息时的数据的流程的图。

图 14 表示在再生系统再生 DVD-ROM 存储盘时的认证步骤和数据传送步骤。

图 15 表示在再生系统再生 DVD-R 存储盘时的认证步骤和数据传送步骤。

图 16 为表示以往的复制控制的原理的图。

图中，101：符合再生装置，102：符合记录装置，105：符合再生装置，301：数字 I/F，302：模拟 I/F，303：密码解读部，304：编码部，306：WM 改写部，307：WM 解码部，308：记录控制部，309：控制部，310：扰频部，311：写入部，313：读出部，314：存储盘类别判别部，401：读出部，402：去扰频部，403：扰频状态检测部，404：存储盘类别判别部，405：控制部，406：WM 解码部，407：再生控制部，408：解码部，409：模拟 I/F，410：加密部，411：数字 I/F。

以下参照附图对基于本发明的加密信息信号、信息记录介质、信息信号再生装置及信息信号记录装置进行说明。在实施例中，信息记录介质为以 DVD-RAM（ROM）为代表的光盘，在此光盘上记录有信息信号。

还有，复制控制的对象为表示图象、声音等的信息信号即音像信息。

在以下的说明中，把记录型 DVD 称为 RAM 盘，把再生专用的 DVD 称为 ROM 盘。还有，把与后述的复制世代限制处理对应的记录装置及再生装置称为符合装置，把不与复制世代限制处理对应的装置称为非符合装置。

实施例 1

图 1 为用于说明基于本实施例的复制世代管理方法的概略图。在本实施例中，在 ROM 盘 100 上记录有音像等信息信号。但是，也可以利用 RAM 盘取代 ROM 盘。

首先对本实施例中的信息信号进行说明。除了表示音像等信号之外，在信息信号中还以噪声的形式嵌入有电子水印信息 WM（digital WaterMark）。电子水印信息的特征主要在于即便对作品（图象和声音）进行改变或进行压缩或扩张处理电子水印信息也不会消失、电子水印信息以不易被人的眼和耳感觉的水平被嵌入以及即便嵌入电子水印信息也能保持原作品的品质。由此特征可以防止非法改写并可以进行再生控制及记录控制。

在信息信号中还记录有复制控制信息（未图示）。复制控制信息为表示能否复制的信息。例如为使用 2 位信息的 CGMS（Copy Generation Management System）。根据 CGMS，“00”表示自由复制，“01”表示可复制 1 次，“10”表示绝对禁止复制，然后，“11”表示“禁止除此以外的复制”。

在把信息信号作为复制控制的对象的情况下，例如在全面禁止对信息信号进行非法复制的情况下，如果不是被正式授权的装置就无法进行信息信号的再生，因此，在本发明中把信息信号扰频（加密）后再记录。本发明特有的处理是把表示信息信号是被扰频后的信息的扰频信息“Scrambled”作为电子水印信息 WM 叠加在信息信号上。因此，扰频信息是可以被用于识别信息信号是否处于被加密的状态的密码状态识别信息。关于使用了电子水印信息的复制控制将在后面进行详细说明。根据上述的电子水印信息的特征，即便对信息信号进行改变或进行压缩或扩张处理扰频信息“Scrambled”也不会消失，因此，可以检测出来。扰

频处理是对要被电子水印信息叠加的信息信号依照特定的扰频方式（加密方式）进行的。

另一方面，在不把信息信号作为复制控制的对象的情况下，例如在允许对信息信号进行自由复制的情况下，信息信号就不被扰频。在此情况下，在信息信号上既可以叠加也可以不叠加电子水印信息。在叠加电子水印信息的情况下，电子水印信息成为表示信息信号没被扰频的扰频信息“non-scrambled”。记录装置（未图示）把没被扰频的信息信号照原样记录在存储盘上或把叠加了电子水印信息的信息信号记录在存储盘上来制造 ROM 盘 100。

在说明本发明的复制世代管理方法之前，先对在制造 ROM 盘 100 时的扰频处理的步骤进行说明。以下说明的扰频处理是 ROM 盘 100 的制造商利用创作系统及盘切割系统进行的。扰频处理的例子为 DVD-ROM 的著作权保护系统 CSS（Content Scramble System）。包含音像等的信息信号是分级地用 3 类密码锁进行加密的。所谓的 3 类密码锁是指标题锁、盘锁及主锁。以下顺着著作权保护系统 CSS 的内容加密步骤进行说明。在本说明书中，称为“扰频”的术语是“加密”的意思。用于扰频的加密方式只要是用一个锁进行加密的算法即可。因此，可以利用众所周知的算法。这里省略对算法的说明。还有，从安全的观点考虑，此算法多数是非公开的。另一方面，把从被扰频的信息恢复到没被扰频的信息称为“去扰频”。这与“解读”或“解码”这样的术语是同义的。

扰频处理的步骤如下。首先，信息信号被以 MPEG 压缩，然后，用标题锁扰频。标题锁为作者比如电影导演对存放在存储盘中的每个标题即信息信号的每个单元自由选择的锁。被扰频的信息信号被存放在盘的数据记录区中。

其次，用盘锁对标题锁加密。所谓盘锁是指著作权管理者比如电影公司可以对每个存储盘自由选择的锁。当存储盘含有 1 个以上的加密标题时，著作权管理者可以自由决定盘锁。被加密了的标题锁是被存放在存储盘的扇区头部区域上的，用户无法存取。

最后，盘锁被用主锁加密并被转换为盘锁集。所谓主锁的指对被扰频的信息信号进行解密的去扰频装置分配给每个制造商的锁，因制造商而

异。所谓“被加密了的盘锁集”是指存在 1 个或多个被加密了的盘锁的意思。这是因为只有被授权的制造商的数目的主锁，因此，与该数目相同的数目的 1 以上的盘锁被生成。被加密了的盘锁集是被存放在存储盘的引导区上的，用户无法存取。

通过以上的处理，被扰频了的信息信号、被加密了的标题锁及被加密了的盘锁集被存放在 ROM 盘 100 上。

为了再生成为复制控制对象的 ROM 盘 100 的信息信号，必须进行扰频处理。为了进行扰频处理，必须接受对于上述规定的加密方式的许可并得到与解码锁（主锁）或解码算法相关的信息。在安装了图 1 所示的解码功能的符合再生装置 101 中，可以从 ROM 盘 100 读出被实施扰频的信息信号并进行去扰频，得到能以 MPEG 解码的信息信号。

下面对 DVD 播放机等再生机器进行的去扰频处理进行说明，然后对 DVD-RAM 驱动器等记录机器进行的扰频处理进行说明。图 2 为表示在对被扰频了的信号信息进行读出或写入时的数据的流程的图。

图 2（a）表示对被记录在存储盘 210 上的被扰频的信息信号进行去扰频处理的概念图。存储盘 210 为相当于 ROM 盘 100 的盘，记录有被扰频了的信息信号 212、被加密了的标题锁 214 及被加密了的盘锁集 216。这里，被扰频了的信息信号 212 设为被以 MPEG 压缩的音像信息。再生机器的去扰频部 220 为对信息信号进行去扰频并进行 MPEG 解码的装置。去扰频部 220 包含有盘锁解码部 222、标题锁解码部 224、信息信号解码部 226 和 MPEG 解码器 228。

去扰频部 220 从存储盘 210 读出被加密了的盘锁集 216、被加密了的标题锁及被扰频了的信息信号。盘锁解码部 222 首先用保存在内部存储区（未图示）的主锁或通过再生机器的其他构成要素所给的主锁从读出的盘锁集 216 对自己的盘锁进行解码。然后，标题锁解码部 224 用解密了的盘锁对被加密了的标题锁 214 进行解码。然后，信息信号解码部 226 用解密了的标题锁对被扰频了的信息信号 212 进行解码。照这样进行去扰频处理。被去扰频了的信息信号是被以 MPEG 压缩处理的数据，因此，在本实施例中，MPEG 解码器 228 进行解码处理并输出音像信息。以上对去扰频部 220 的处理进行了说明。

图 2（b）表示为了在存储盘 230 上进行记录而对信息信号进行扰频处理的概念图。此处理为在比如为在记录“可复制 1 次”的信息信号时的处理。被用于写入的存储盘 230 记录有制造商在出厂时预加密的盘锁集 236。

首先，扰频部 240 的 MPEG 编码器 248 对被输入的信息信号进行 MPEG 压缩处理并把生成的 MPEG 数据送到信息信号加密部 246。其次，信息信号加密部 246 用标题锁对 MPEG 数据进行扰频处理。标题锁为由随机数发生器 250 产生的随机数。然后，此标题锁用盘锁在标题锁加密部 244 上被加密，并作为被加密了的标题锁 234 记录在存储盘 230 上。盘锁用扰频部 240 所保存的主锁对被记录在存储盘 230 上的被加密了的盘锁集 236 进行解密。

当再一次生成标题锁并作为被加密了的标题锁 234 记录在存储盘 230 上时，在其后进对信息信号进行扰频处理并记录时用到被记录并被加密了的标题锁 234。也就是说，扰频部 240 读出存储盘的被加密了的标题锁 234 并用盘锁进行解密，再用标题锁对信息信号进行扰频。

如上所述，扰频部 240 可以通过 2 条路径取得标题锁。也就是说，有取得由随机数发生器 250 产生的随机数作为标题锁的情形和对记录在存储盘 230 上的被加密了的标题锁 234 进行解密并取得作为标题锁的情形这 2 种情形。将来在节目配送增加时，可以考虑在播放业者（内容制作者）这边生成标题锁，以该标题锁被扰频的信息信号作为数字播放由无线电波配送。在次情况下，把由播放业者取得的标题锁和被扰频的信息信号记录在存储盘上。

象以上那样进行信息信号的扰频处理及去扰频处理。

下面，再参照图 1 对基于本发明的复制世代管理的原理进行说明。在本实施例中，在把信号信息作为复制控制的对象的情况下，扰频信息“Scrambled”作为电子水印信息叠加在该信号信息上。被扰频信息“Scrambled”叠加的信号信息被扰频并被记录在 ROM 盘 100 上。

基于本发明的复制世代管理的主要特征在于把存储盘上的信号信息的扰频状态（即是否被扰频）和扰频信息的状态（即扰频信息是否为“Scrambled”）进行比较，根据比较结果决定是否进行再生或记录及是

否对此进行限制。判断信号信息是否被扰频、信号信息或相关的附属文件的信息之中规定的标志是否显现、或去扰频部是否正常工作。

以下进行具体说明。首先，再生装置 101 先从 ROM 盘 100 读出被扰频的信号信息并进行去扰频。然后，再生装置 101 从被去扰频了的信号信息检测出扰频信息并比较扰频状态是否一致。这里，当信号信息处于被扰频的状态且扰频信息为“Scrambled”时可以判断为扰频状态是一致的。由此，符合再生装置 101 输出去扰频了的信息信号。此时应该注意的是在输出的信息信号中叠加有扰频信息“Scrambled”。作为电子水印信息的扰频信息不会因符合再生装置 101 的去扰频处理而消失。

接着，说明在想把从再生装置输出的信息信号非法记录在记录介质的情况下限制记录的原理。符合记录装置 102 从符合再生装置 101 接受被去扰频了的信息信号。符合记录装置 102 确认所接受的信号信息处于去扰频状态以及叠加的扰频信息为“Scrambled”。结果，由于输出信息信号的状态与表示扰频信息的状态不一致，因此，符合记录装置 102 不往 RAM 盘等记录介质上记录。由此，可以在符合记录装置 102 中限制信号信息的记录。

另一方面，当在信息信号上没被实施扰频时，同样，只要比较扰频状态即可。在电子水印信息没被检测出的情况下或电子水印信息“Non-Scrambled”被检测出的情况下进行信息信号的输出。只要输出的信号是可以自由复制的，在符合记录装置 102 中，允许往 RAM 盘复制信息信号。

下面对在信息信号被非法复制到 RAM 盘上的情况下限制再生的原理进行说明。非符合记录装置 103 接受符合再生装置 101 输出的被去扰频了的信息信号。此信息信号带有扰频信息“Scrambled”，虽然是复制控制对象，但非符合记录装置 103 没检测出电子水印信息，因此，把信息信号复制往 RAM 盘 104。然后，当要在符合再生装置 105 上再生这样的 RAM 盘 104 时，符合再生装置 105 对扰频状态进行比较。在此情况下，信息信号以被扰频的状态被记录，另一方面，在信息信号上叠加有表示被扰频的扰频信息“Scrambled”。因此，符合再生装置 105 从比较结果的不一致判断 RAM 盘 104 的信息信号为非法复制的信息信号。由此，

符合再生装置 105 禁止信息信号的再生。

还有，即使在记录对象不是 RAM 盘 104 的情况下也对再生进行限制。例如，记录对象也可以是可以写入但写入后成为只读盘的 DVD-R。

为了更加可靠地禁止非法记录及再生，还并用这样的手法，即扰频时根据记录介质的类别的不同使所用的加密算法也不同。例如，通过使用于 DVD-ROM 的加密算法和用于 DVD-RAM 的加密算法不同，即便把以 DVD-ROM 用的加密算法扰频的信息信号从 DVD-ROM 非法复制到 DVD-RAM 也可以禁止从 DVD-RAM 再生。为了实现此工作，例如也可以设置一个使记录介质的类别和用于各类别的加密算法对应的表。在去扰频电路用与记录介质的类别对应的解密算法无法去扰频的情况下，可以禁止从非法复制的记录介质再生信号信息。表示记录介质的类别的类别信息也可以和扰频信息一起作为电子水印信息叠加到信息信号上。类别信息是表示被记录的记录介质的种类的。因此，可以区别在 DVD-R 上记录的情形和在 DVD-RAM 上记录的情形。

如上所述，在本发明中，在被扰频（加密）了的信息信号上叠加有作为电子水印信息的表示该信息信号被加密的加密信息（扰频信息“Scrambled”）。即便在信号信息被解密了的情况下，电子水印信息也不被改变而以原来的内容留下。因信号信息表示解密状态、电子水印信息表示加密状态，因此，通过检测出此不一致可以在符合记录装置及再生装置上禁止往别的记录介质进行非法复制或禁止从非法的记录介质再生。因此，即使不把电子水印信息的改写部装在符合再生装置上也可以禁止在符合再生装置上再生用非符合记录装置 103 制作的非法复制盘。

还有，在本实施例中，把被给予信息信号的扰频信息（“Scrambled”、“Non-Scrambled”）作为电子水印信息叠加在信息信号上，但只要是表示信息信号的扰频状态的，也可以用其他信息。例如，在 ROM 盘中，对于作为复制控制信息的“绝对禁止复制”的信息信号，在对信息信号扰频并记录的情况下，即便把此复制控制信息作为电子水印信息叠加在信息信号上也可以得到同样的效果。

[记录装置]

下面参照图 3 对符合记录装置 102 的构成进行说明。图 3 表示符合记

录装置 102 的构成。符合记录装置 102 具备有数字输入端子 301 和模拟输入端子 302。各端子分别从与其连接的机器接收密码锁信息等数字信号和音像信息等模拟信号。密码解读部 303 根据从被连接在数字输入端子上的机器送来的密码锁信息对加密了的数据进行解密，还原压缩视频数据。此时，检测出表示被输入的信息信号是否为可复制的信号的复制控制信息。复制控制信息也是被叠加在信息信号上的信息。

还有，通过模拟输入端子 302 被输入的影象信息通过模拟输入端子 302 供给编码部 304 并被进行 MPEG 压缩。其结果生成影象压缩数据。此时，检测出表示被输入的信息信号是否为可复制的信号的复制控制信息。

选择器 305 根据与用户的输入选择相应的选择控制信号选择输出来自密码解读部 303 的数据或来自编码部 304 的数据。

由此选择器 305 输出的数据通过 WM 改写部 306 供给记录控制部 308。WM 改写部 306 所进行的处理是为了把扰频信息“Scrambled（RAM）”作为电子水印信息叠加在信息上。但是，此处理必须在进行了后面要说明的记录介质的类别判别后进行。WM 改写部 306 的处理用比如模拟噪声编码序列的编码对扰频信息进行频谱展开并输出频谱展开后的扰频信息。这是众所周知的技术，因此，省略详细的说明。由选择器 305 输出的数据还供给 WM 解码部 307。WM 解码部 307 抽出作为电子水印信息被叠加在信息信号上的扰频信息并判别记载内容，然后把判别输出供给控制部 309。

控制部 309 根据从输入信息检测出的复制控制信息及电子水印信息判别输出判别是否可能对输入信息进行记录（复制），在判别为可以记录（复制）的情况下，还要判别是否需要为了控制复制而进行电子水印信息的改写。然后，当判别为禁止记录时，控制部 309 控制记录控制部 308 使之不执行记录。还有，当判别为可以记录或可以复制 1 次时，控制部 309 使记录控制部 308 执行记录。此时，记录装置 102 通过读出部 313 读出与存储盘的类别（RAM 盘、只可写 1 次的盘等类型）相关的信息，并通过存储盘类别判别部 314 判别该存储盘的类别。其结果决定如前面所说明的扰频信息的内容，在 WM 改写部 306 上生成应叠加在信息信号上的扰频信息并在记录控制部 308 中被叠加在信息信号上。借助于扰频部

310，信息信号根据其存储盘的类别被实施特定的扰频并通过写入部 311 被记录在 RAM 盘 312 上。

下面参照图 4 对在符合记录装置 102 结束了密码解读后的处理进行说明。图 4 为表示记录装置 102 的记录处理流程的流程图。

首先在输入信息信号时检查检测出的复制控制信息（步骤 S101）。然后判别复制控制信息是否为“Never Copy”（绝对禁止复制）或“No more Copy”(禁止除此以外的复制)（步骤 S102）。在是其中任何一种信息的情况下禁止记录并中止记录处理（步骤 S103）。还有，所谓“Never Copy”（绝对禁止复制）是表示这样的限制，即信息信号的复制被完全禁止。另一方面，“No more Copy”(禁止除此以外的复制)是表示这样的限制，即在只可复制 1 次的音乐数据和图象数据被复制的情况下除这 1 次以外的信息信号的复制被禁止。

在不是其中任何一种信息的情况（既不是“Never Copy”也不是“No more Copy”的情形）下，检查被叠加在输入信号上的电子水印信息（WM）的判定输出（步骤 S104），并判别电子水印信息（WM）是否处于“Scrambled”的状态（步骤 S105）。如果是处于“Scrambled”的状态，则表明想要记录的信息信号是原先被扰频了的信息，由此判断此信息信号是非法修改复制控制信息后的信息并中止记录处理（步骤 S103）。如果不是处于“Scrambled”的状态则可以判断为是可记录的信息。

当判断为是可记录的信息时，接着，为了判断是否需要对该信息信号进行扰频，判断复制控制信息是否为处于“只可复制 1 次（One Copy）”的状态的信息信号（步骤 S106）。如果是处于“只可复制 1 次的状态，则把电子水印信息改写为“Scrambled（RAM）”状态（步骤 S107），并依照特点的扰频方式进行扰频处理（步骤 S108）。记录装置 102（图 3）这样生成并把信息记录在 RAM 盘上（步骤 S109）。

如果不是处于“只可复制 1 次”的状态（复制多少次也还是“可复制”的情形），则不进行扰频处理就记录在 RAM 盘上（步骤 S109）。

通过以上那样的符合记录装置 102 被记录的 RAM 盘对于复制控制所必需的“只可复制 1 次”的信息信号使作为电子水印信息的扰频信息和对信息信号的扰频成对被记录。

还有，存储盘类别判别部 214 也可以根据读出部 213（图 2）所读出的规定信息判别所装的存储盘的种类并把存储盘类别记录在电子水印信息上。存储盘类别有 ROM 盘（只读）、RAM 盘（可写入）、只可写入 1 次的盘、可写入 1000 次左右的盘、可写入 10 万次左右的盘等。存储盘的判别是根据记录了盘的物理特性（聚焦特性、跟踪特性、再生特性）和存储盘类别的控制区的信息等进行的。

还有，关于扰频处理，也可以考虑信息再生时的负载而只把一部分信息（MPEG 压缩数据的 I 帧数据等）作为扰频对象。在此情况下，电子水印信息必须完全叠加在该部分信息上。

还有，在想要制作对上述那样的信息信号进行了扰频的 ROM 盘的情况下，信息记录装置比如作为创作系统及盘切割系统被构成。创作系统根据信息信号进行信息信号的压缩处理，同时，把扰频信息作为电子水印信息进行叠加。盘切割系统根据信息信号进行扰频处理并制成存储盘原盘。这样就可以制成如上述那样的可控制复制的 ROM 盘。

[再生装置]

下面参照图 5 对符合再生装置 105 的构成进行说明。还有，符合再生装置 105 具有和符合再生装置 101 相同的构成。图 5 表示符合再生装置 105 的构成的方框图。被记录在装在再生装置 105 上的存储盘上的信息被读出部 401 读出并被供给去扰频部 402、扰频状态检测部 403 及存储盘类别判别部 404。

扰频状态检测部 403 抽出作为附加信息被记录在存储盘上的扰频标记、检测出记录信息上是否有扰频并把该检测结果输出到控制部 405。还有，在禁止复制的 ROM 盘上加有特定加密方式（比如 CSS：Content Scramble System 方式等）的密码。

存储盘类别判别部 404 判别所装的存储盘的类别并该判别结果供给控制部 405。存储盘类别有 ROM 盘（只读）、RAM 盘（可写入）、只可写入 1 次的盘、可写入 1000 次左右的盘、可写入 10 万次左右的盘等。存储盘的判别是根据记录了盘的物理特性（聚焦特性、跟踪特性、再生特性）和存储盘类别的控制区的信息等进行的。

去扰频部 402 在 ROM 盘的情况下解读由出厂商实施的扰频、在 RAM

盘的情况下解读由记录装置的扰频部 240（图 2（b））实施的扰频。去扰频部 402 进行参照图 2（a）说明的去扰频部 220 的处理。

去扰频部 402 把输出数据供给 WM 解码部 406 和再生控制部 407。WM 解码部 406 对作为电子水印信息被叠加在信息信号上的扰频信息进行解密。所谓“解密”是表示抽出扰频信息并判别其内容。这是因为电子水印信息是被考虑作为噪声被叠加在信息信号上并被编码的。WM 解码部 406 把判别结果输出到控制部 405。

控制部 405 根据对这些存储盘类别的的判别结果、扰频标记及对电子水印信息的判别输出决定是允许还是禁止再生。在符合记录装置 102（图 1）所记录的存储盘中，对信息信号的扰频和扰频信息所表示的内容成对地被记录。

因此，在装上非法的存储盘的情况下，去扰频部 402 把禁止再生的控制信息供给再生控制部 407 并禁止此再生控制部 407 的后续处理。在是从正式的存储盘而来的信息信号的情况下，再生控制部 407 的后续处理有效。再生控制部 407 把音像信息供给解码部 408，解码部 408 把被以 MPEG 压缩的数据展开（解码）。模拟 I/F409 对被展开解码了的数据进行 D/A 转换并供给外部机器。还有，在有被连接到数字 I/F411 的机器的情况下，加密部 410 对以 MPEG 压缩的数据进行加密并从数字 I/F411 输出。

下面参照图 6 对符合再生装置 105（图 5）的再生处理进行说明。图 6 为表示再生处理流程的流程图。在符合再生装置 105（图 5）中，首先判别被记录在所装的存储盘上的信息信号上是否加有扰频（步骤 S201）。在扰频中有被加在记录装置 102 的扰频部 240（图 2）上的 RAM 盘用的扰频方式和 ROM 盘用的扰频方式（比如 CSS 方式）。扰频方式因存储盘的类别而异，因此，存储盘类别判别部 404（图 5）检查存储盘的类别（步骤 S202）。

在存储盘类别的检查结果为 ROM 盘的情况下，去扰频部 402（图 5）进行 ROM 用的去扰频处理（步骤 S203）。接着，WM 解码部 406（图 5）检查在被去扰频了的信息信号上是否记载有表示扰频状态的电子水印信息（WM）（步骤 S204），控制部 405（图 5）判别电子水印信息是否处

于“Scrambled（ROM）”的状态（步骤 S205）。当处于“Scrambled（ROM）”的状态时，控制部 405（图 5）允许再生（步骤 S211），不处于该状态时禁止再生（步骤 S212）。

同样，在步骤 S202 中的存储盘类别的检查结果即存储盘为 RAM 盘的情况下，去扰频部 402（图 5）进行 RAM 用的去扰频处理（步骤 S206）。接着，WM 解码部 406（图 5）从被去扰频了的信息信号上检测出表示扰频状态的电子水印信息（WM）（步骤 S207），控制部 405（图 5）判别电子水印信息是否处于“Scrambled（RAM）”的状态（步骤 S208）。当处于“Scrambled（RAM）”的状态时，控制部 405（图 5）允许再生（步骤 S211），不处于该状态时禁止再生（步骤 S212）。

还有，当在步骤 S201 中判断为没加扰频时，去扰频部 402（图 5）不进行去扰频处理而把信号信息发送到 WM 解码部 406（图 5）。WM 解码部 406（图 5）检测出电子水印信息（WM）（步骤 S209），控制部 405（图 5）判别电子水印信息是否处于“Scrambled”的状态（步骤 S210）。当处于“Scrambled”的状态时，控制部 405（图 5）禁止再生（步骤 S212），不处于该状态时允许再生（步骤 S211）。这里所谓的“不处于该状态时”是指电子水印信息没被检测出时或检测出的电子水印信息为“Non-Scrambled”之时。

具体来说，如果是由符合记录装置 102（图 1）所记录的存储盘，则在电子水印信息被记录为“Scrambled”的信息信号上进行扰频处理。尽管在电子水印信息上记录有“Scrambled”，但是，如果信号信息没被扰频则意味着该信息信号是被非法复制的。例如，符合再生装置 101（图 1）的输出被非符合记录装置 103（图 1）记录在存储盘上的情形、或对被加在信息信号上的扰频进行非法去扰频并记录在存储盘上的情形就是这样。

另一方面，如果使用基于上述那样的本发明的记录装置 102（图 1、图 3）及再生装置 101、105（图 1、图 5），则可以禁止在此情况下的再生。由此，即使不在再生装置上安装用于改写电子水印信息的改写机构也可以防止非法复制，降低再生装置的成本变得容易了。

还有，在只有一部分的信息信号被扰频的情况下，不仅要检查信息信

号的扰频标记，还要检查在去扰频部 402 上去扰频处理是否正常进行。由此，即使非法地把非法复制的信号的扰频标记改写为扰频状态也可以禁止再生。这里，通过扰频对信息信号进行了加密，但如果用其他方式进行加密也可以得到同样的效果。

还有，在实施例 1 中对把光盘用作信息记录介质的情形进行了说明，但对于其他的半导体存储器和磁记录介质（硬盘等）也是一样。

实施例 2

在实施例 1 中，记录装置 102（图 1、图 3）及再生装置 101、105（图 1、图 5）把信息信号往存储盘上记录或从存储盘再生信息信号的模块（写入部 311（图 3）、读出部 401（图 5））、检测电子水印信息的模块 [WM 解码部 307（图 3）、406（图 5）]、展开/压缩信息信号的模块 [编码部 304（图 3）、解码部 408（图 5）]全部都包含在装置内部，此实施例对这样的构成进行了说明。

但是，在用 PC 实现记录装置和再生装置的情况下，一般都把对信息信号进行记录/读出的驱动部和编码/解码部各自作为另外的装置构成。

在作为另外的装置构成的情况下，解码部根据用驱动部检测出的存储盘的类别进行再生控制，因此，存储盘类别被非法替换并进行了非法复制的存储盘可以进行再生。具体来说，在通过非符合记录装置把被记录在 ROM 盘上的信息信号记录在 RAM 盘上、然后进行再生的情况下，通过在驱动部和解码部之间介入非法软件可以把驱动部检测出的存储盘的类别偷换为“ROM”。结果，在往 RAM 盘上非法复制 ROM 盘的情况下，无法象符合再生装置 101、105（图 1）那样防止再生。本实施例对即便在这样的情况下也可以防止再生的构成进行说明。

[通过 PC 的记录装置]

图 7 为表示通过个人计算机（PC）记录系统 600 实现符合记录装置的例子的图。如图 7 所示，这样的符合 PC 记录系统 600 主要由 PC 编码器 600-1 和 PC 记录装置（驱动）600-2 构成，其间用可防止非法复制的数字 I/F（SCSI 或 ATAPI、IEEE1394 等）连接。PC 编码器 600-1 相当于符合记录装置 102（图 3）中从 I/F301、302（图 3）到扰频部 310（图 3）的构成并进行相同的动作。因此，省略与共同的动作相关的说明。另一

方面，PC 记录装置（驱动）600-2 相当于写入部 311（图 3）的构成。

下面对 PC 编码器 600-1 的动作和由符合记录装置 102（图 3）中从 I/F301、302（图 3）到扰频部 310（图 3）的构成所实现的动作的不同点进行说明。在把可复制 1 次的信息信号记录在 RAM 盘上的情况下，PC 编码器 600-1 的扰频部 610 对该信息信号进行特定的扰频。此时，由于在 PC 记录驱动和 PC 编码器之间安全地共享成为扰频的基础的锁信息，因此，认证部 613、617 通过数字 I/F615、616 互相进行认证。在认证成立的情况下，可以确认在认证部 613 和 PC 记录驱动中的认证部 617 之间互相接受正式的许可证的装置即为符合的装置。在认证成立的情况下，还共享用于加密在数字 I/F 上传输的数据的总线锁。这样，使用共享化了的总线锁在 PC 编码器中对在加密部 614 中需要保护的数据（锁信息和信息信号等）进行加密，把被加密了的数据通过数字 I/F615 发送到 PC 记录驱动 600-2。

PC 记录驱动 600-2 的密码解读部 618 根据共享了的总线锁对接收的数据进行解码。写入部 611 把从 PC 编码器 600-1 接收的信息信号记录在 RAM 盘 612 上。此时，只要对 PC 编码器的认证不成立，记录控制部 619 就进行记录控制，不把锁信息等需要记录在特定的保护区中的数据写入 RAM 盘 612 上。

在符合装置中，借助于存储盘类别和所记录的信息信号改变相互认证方式和对锁信息和信息信号的处理方法。PC 记录驱动 600-2 的存储盘类别判别部 621 根据从读出部 620 再生的信号判别存储盘 612 的物理特性（聚焦特性、跟踪特性、再生特性）和记录在存储盘 612 的控制区上的存储盘类别。判别结果被输出到控制部 622。还有，表示存储盘类别的信息有可能在传输过程中被改动。但是，根据后述的手法可以防止这样的传输过程中的改动。在控制部 622 中，对照着存储盘类别转换认证方式、数据的传输方式等并和 PC 编码器 600-1 进行数据传输。

下面对 PC 记录系统 600 的 PC 编码器 600-1 及 PC 记录驱动 600-2 的处理流程进行说明。图 8 为表示在 PC 编码器 600-1 的控制部 609（图 7）上的处理流程的流程图。首先，在复制只可复制 1 次的信息信号的情况下，控制部 609（图 7）使得在认证部 613 和 PC 记录驱动 600-2 的认证

部 617（图 7）之间进行相互认证（步骤 S301）。根据认证部 613（图 7）的认证的结果，控制部 609（图 7）判别双方是否为符合装置（步骤 S302）。由此可以确认在记录信息信号之前是否为正式接受了许可证的机器。

在认证成立的情况下，生成在 PC 编码器 600-1 和 PC 记录驱动 600-2 之间共享的总线锁（步骤 S303）。然后，PC 编码器 600-1（图 7）从 PC 记录驱动 600-2 取得用于由 PC 记录驱动 600-2（图 7）生成的扰频的锁信息（以下称为“扰频锁信息”）（步骤 S304）。扰频锁信息为 PC 记录驱动 600-2 根据共享的总线锁进行加密及/或防改动处理并传输的信息。

在 PC 编码器 600-1 的控制部 609（图 7）中依照与图 4 一样的记录流程进行信息信号的记录（步骤 S305 以后的步骤）。已经参照图 4 说明了此记录流程，因此省略其说明。

与图 4 的流程不同之处在于在进行了步骤 S106（图 4）的“只可复制 1 次”的判别后插入检查相互认证是否成立的步骤 S311。在步骤 S311 中相互认证不成立的情况下禁止记录。

接着对 PC 记录驱动 600-2（图 7）的处理进行说明。图 9 为表示在 PC 记录驱动 600-2 的控制部 622（图 7）上的处理流程的流程图。与前面的 PC 编码器 600-1 一样，在记录只可复制 1 次的信息信号的情况下，控制部 622（图 7）使得在认证部 617 和 PC 编码器 600-1 的认证部 613（图 7）之间进行相互认证（步骤 S401）。然后，根据认证部 617（图 7）的认证的结果，控制部 622（图 7）判别相互认证是否成立（步骤 S402）。

在认证成立的情况下，控制部 622（图 7）生成共享的总线锁。然后控制部 622（图 7）根据共享的总线锁对扰频锁信息进行加密及/或防改动处理，并从 PC 记录驱动 600-2（图 7）传输到 PC 编码器 600-1（图 7）（步骤 S404）。然后，允许对被扰频的信息信号及扰频锁信息和扰频控制信息等进行存取（记录或再生）并进行记录（步骤 S405）。另一方面，在步骤 S402 中相互认证不成立的情况下，只允许记录信息信号，禁止往存储盘的一部分的特定区域记录扰频锁信息、扰频控制信息等（步骤 S406）。

因此，在 PC 编码器 600-1 和 PC 记录驱动 600-2（图 7）不是符合关系的情况下，可以防止对扰频锁信息和扰频控制信息等进行存取。结果，

在记录控制复制所必需的可复制 1 次的信息信号时，在组合双方为符合的 PC 编码器 600-1 和 PC 记录驱动 600-2 的符合 PC 记录系统 600（图 7）中，电子水印信息“Scrambled”和对信息信号的扰频状态被检测出，复制成为可能。另一方面，在 PC 编码器和 PC 记录驱动的某一方为非符合的 PC 系统中，无法对存储盘上的特定区域进行存取，因此，不能进行正确的扰频。

[通过 PC 的再生装置]

图 10 为表示通过个人计算机（PC）再生系统 900 实现符合再生装置的例子的图。如图 10 所示，这样的符合 PC 再生系统 900 主要由 PC 解码器 900-1 和 PC 再生装置（驱动装置）900-2 构成，其间用可防止非法复制的数字 I/F（SCSI 或 ATAPI、IEEE1394 等）连接。PC 解码器 900-1 相当于符合生装置 101、105（图 5）中从去扰频部 402（图 5）到 I/F409、411（图 5）的构成并进行相同的动作。因此，省略与共同的动作相关的说明。另一方面，PC 再生装置（驱动）900-2 相当于读出部 401（图 5）的构成。读出部 901 从装在此 PC 再生装置（驱动）900-2 上的存储盘 905 读出记录的信息并供给扰频状态检测部 904 及存储盘类别判别部 903。扰频状态检测部 904、存储盘类别判别部 903 与符合生装置 101、105（图 5）的情形一样获得扰频标记及存储盘类别。

PC 再生装置（驱动）900-2 的认证部 915 在从数字 I/F916 输出被实施扰频的信息信号的情况下和 PC 解码器 900-1 的认证部 919 之间进行相互认证。在认证不成立的情况下，再生控制部 913 禁止从 PC 再生驱动部读出信息信号。在认证成立的情况下，PC 编码器中的去扰频部 902 读出信息信号并对被实施了扰频的禁止复制的信息信号进行特定的去扰频处理。

此时，由于在 PC 再生驱动和 PC 编码器之间安全地共享成为扰频的基础的锁信息，因此，认证部 915、919 通过数字 I/F916、917 互相进行认证。在认证成立的情况下，可以确认在认证部 915 和认证部 919 之间为互相接受正式的许可证的装置。具体来说，在正常认证成立的情况下，还共享用于加密在数字 I/F 上传输的数据的总线锁。这样，使用共享化了的总线锁在 PC 再生装置（驱动）900-2 中对在加密部 914 中需要保护

的数据（锁信息和信息信号等）进行加密，把被加密了的数据通过数字I/F916发送到PC解码器900-1。

在符合装置中，借助于存储盘类别和所记录的信息信号改变相互认证方式和对锁信息和信息信号的处理方法。存储盘类别判别部903根据读出部901的再生信号从记录了物理特性（聚焦特性、跟踪特性、再生特性）和存储盘类别的控制区等判别存储盘类别。判别结果被输出到控制部912。在控制部912中，对照着存储盘类别转换认证方式、数据的传输方式等并和PC解码器900-1进行数据传输。对PC解码器900-1也一样，对照着记录了再生的信息信号的存储盘类别和信息信号的扰频方式转换认证方式、数据的传输方式等。

PC解码器900-1的密码解读部918根据共享了的总线锁对接收的数据进行解码。从去扰频部902到I/F部909、911的处理与符合生装置101、105（图5）的情形相同，因此省略其说明。

PC解码器900-1的控制部905不仅根据信息信号的扰频（有无扰频和扰频方式）及作为电子水印信息的扰频信息进行再生控制，还利用认证方式和数据传输方式进行再生控制。

下面对PC再生系统900的PC解码器900-1及PC再生装置（驱动）900-2的处理流程进行说明。图11为表示在PC驱动900-2的控制部912（图10）上的处理流程的流程图。首先，当再生被扰频并被记录在存储盘上的信息信号时，控制部912（图10）使得在认证部915和PC解码器900-1的认证部919（图10）之间进行相互认证（步骤S501）。根据认证部915的认证的结果，控制部912（图10）判别双方是否为符合装置（步骤S502）。由此可以确认在记录信息信号之前是否为正式接受了许可证的机器。

在认证成立的情况下，生成在PC解码器900-1和PC驱动900-2（图10）之间共享的总线锁（步骤S503）。然后，控制部912（图10）根据共享的总线锁对扰频锁信息进行加密及/或防改动处理并从PC驱动900-2（图10）传输到PC解码器900-1（图10）（步骤S504）。然后，允许对被扰频的信息信号及扰频锁信息和扰频控制信息等进行存取并进行再生（步骤S505）。另一方面，在步骤S502中相互认证不成立的情况下，只

允许再生信息信号，禁止从存储盘的一部分的特定区再生信息（步骤S506）。

图12为表示PC解码器900-1的控制部905的处理流程的流程图。与前面的PC驱动900-2一样，当再生被扰频并被记录在存储盘上的信息信号时，控制部905（图10）使得在认证部919和认证部915之间进行相互认证（步骤S601）。然后，根据认证部919的认证的结果，控制部905（图10）判别相互认证是否成立（步骤S602）。

在认证成立的情况下，生成在PC解码器900-1和PC驱动900-2（图10）之间共享的总线锁（步骤S603）。然后，PC解码器900-1（图10）从PC驱动900-2（图10）取得由PC驱动900-2（图10）生成的扰频锁信息（步骤S604）。

在PC解码器900-1的控制部905（图10）中，与图6一样依照所示的再生流程进行信息信号的再生（步骤S605以后的步骤）。已经参照图6说明了此再生流程，因此省略其说明。

与图6的流程不同之处在于在进行了步骤S202（图6）的存储盘类别判别后变为对与各自的存储盘对应的相互认证是否成立进行检查（步骤S609、S612）。在ROM或RAM用的相互认证不成立的情况下，这样的信息信号的再生被禁止。

因此，在PC解码器900-1和PC驱动900-2（图10）不是符合关系的情况下，可以防止对扰频锁信息和扰频控制信息等进行存取。结果，当再生控制复制所必需不可复制的信息信号时，在组合双方为符合的PC解码器900-1和PC驱动900-2（图10）的PC再生系统900（图10）中，对信息信号的扰频状态和电子水印信息“Scrambled”被检测出。在非符合的PC系统中，无法从存储盘上的特定区域进行再生，可以防止正式的去扰频。

[存储盘类别传送方式]

下面参照图13对不改变存储盘类别而从PC驱动部传输到编码器和解码器的方法进行详细说明。图13为表示在传送存储盘类别的信息时的数据的流程的图。PC驱动部为PC驱动600-2（图7）或PC驱动900-2（图10）。

在 PC 编码器或 PC 解码器中，利用存储盘类别准许信息信号的记录再生。因此，不需要把表示存储盘类别的信息从驱动部改动到编码部或解码部中传输。PC 编码器或 PC 解码器为比如 PC 编码器 600-1（图 7）或 PC 解码器 900-1（图 10）。

在图 13 的存储盘 1250 中记录有用于驱动部和编码器/解码器之间的相互认证的认证锁信息 1201。认证锁信息 1201 为 1 个或多个加密认证锁（EAK1、EAK2、•••）的集合。加密认证锁为用于相互认证的公用锁（认证锁）和记录有认证锁信息的存储盘的类别等由设备锁加密的锁。设备锁为配给各个装置的锁。

下面表示加密认证锁的例子。

EAK1=ENC（设备锁（DK1），{认证锁（AK）、存储盘类别（DT）}）

EAK2=ENC（设备锁（DK2），{认证锁（AK）、存储盘类别（DT）}）

PC 驱动的认证部 915 从由存储盘 1250 读出的认证锁信息取出被分配给机器的加密认证锁（EAK1），并用自有的设备锁 DK1 进行解码。结果得到认证锁（AK）和存储盘类别（DT）。PC 驱动从记录了所装的盘的物理特性（聚焦特性、跟踪特性、再生特性）和存储盘类别的控制区等判别存储盘类别（DT'）。相互认证使用对认证锁（AK）和来自存储盘类别判别部 1202 的存储盘类别（DT'）通过特定的运算（例如在图中为加法）而得到的认证锁（DAK'）。

另一方面，在 PC 编码器/PC 解码器中，从由存储盘 1250 读出的认证锁信息取出被分配给机器的加密认证锁（EAK2），并用自有的设备锁 DK2 进行解码。结果得到认证锁（AK）和存储盘类别（DT）。为了相互认证，使用对认证锁（AK）和存储盘类别（DT）通过特定的运算（例如在图中为加法）而得到的认证锁（DAK）。

这样，用共享了的存储盘认证锁进行相互认证。也就是说，在 DAK=DAK'的情况下相互认证成立，在 DAK≠DAK'的情况下相互认证不成立。即认证部 915 即 919 在其认证锁信息的 DT 和驱动部检测出的 DT'不一致时可以使认证不成立。结果，即使把从 ROM 盘得到的信息信号非法复制到 RAM 盘，认证锁信息中的存储盘类别（DT）和驱动部检测出的 DT'也不一致。因此，相互认证不成立，可以防止信息信号的再

生。还有，即使非法替换认证锁信息，认证锁或存储盘类别也不一致，相互认证不成立。

还有，对在认证锁信息上加密认证锁或存储盘类别并记录的情形进行了说明。但是，在认证锁信息上不包含存储盘类别，即便用这样的方法、即加密由驱动部检测出的存储盘类别并传输到 PC 编码器或解码器中并解密得到存储盘类别，也可以安全传送存储盘类别。因此实际上可以进行正常的信息信号的再生。在认证锁信息上不包含存储盘类别的情况下相互认证不依赖于存储盘的类别而共用，因此，相互认证不依赖于存储盘的类别而成立。但是，即使相互认证成立，在用错误的存储盘类别（扰频方式）再生信息信号的情况下也可以使图象和声音显示得不正确。

根据上述那样的记录装置或再生装置，即使在 PC 驱动部不安装 WM 检测部和 WM 改写部也可以防止非法复制盘的再生。

下面对根据存储盘类别改变认证方式和数据传输方式（数据和锁信息的传输步骤）的处理进行说明。如果反过来利用此性质，也可以从进行认证的处理步骤进行存储盘类别的判别。以下的说明是对于可以作为 PC 驱动部和 PC 解码器利用的系统的。

图 14 表示在再生系统 1400 再生 DVD-ROM 盘 1450 时的认证步骤和数据传送步骤。首先说明总线认证步骤。MPEG 解码器模块 1428 生成随机数 cl，并作为询问数据（drv_chal(c1)）设在 DVD 驱动 1400-1 上。DVD 驱动 1400-1 用作为秘密信息的函数 f 生成 f(c1)并作为应答数据（drv_res(f(c1))）返回 MPEG 解码器模块 1400-2。MPEG 解码器模块 1400-2 用作为自有的秘密信息的函数 f 生成 f(c1)。然后，MPEG 解码器模块 1400-2 检查 f(c1)是否与从 DVD 驱动 1400-1 返回的应答数据一致，然后，MPEG 解码器 1428 确认 DVD 驱动 1400-1 为符合的机器。

接着，DVD 驱动 1400-1 生成随机数 c2，并作为询问数据设在 MPEG 解码器模块 1400-2 上（dec_chal(c2)。MPEG 解码器模块 1400-2 用作为秘密信息的函数 f 生成 f(c2)并作为应答数据返回 DVD 驱动 1400-1（drv_res(f(c2))）。DVD 驱动 1400-1 用作为自有的秘密信息的函数 f 生成 f(c2)。然后，DVD 驱动 1400-1 检查 f(c2)是否与从 MPEG 解码器模块 1400-2 返回的应答数据一致，然后，DVD 驱动确认 MPEG 解码器为符

合的机器。结果，秘密的随时间变化的锁在 DVD 驱动 1400-1 和 MPEG 解码器模块 1400-2 之间共享。

接着对使用了随时间变化的锁的锁信息的秘密传送步骤进行说明。DVD 驱动 1400-1 使用共享了的随时间变化的锁对记录在 DVD-ROM 盘 1450 上的加密盘锁集和加密标题锁进行总线加密并传送到 MPEG 解码器模块 1400-2。在 MPEG 解码器模块 1400-2 中，使用共享了的随时间变化的锁对接收到的被进行总线加密了的加密盘锁集和加密标题锁进行总线解码。

关于对被扰频的信息信号的解码，MPEG 解码器模块 1400-2 利用被进行总线解码了的加密盘锁集和加密标题锁，如图 2（a）所示那样对被扰频了的信息信号进行解码，可以得到作为内容的信息信号。

图 15 表示在再生系统 1500 再生 DVD-ROM 盘 1550 时的认证步骤和数据传送步骤。首先，总线认证步骤与再生上述 DVD-ROM 盘 1450（图 14）时的认证步骤一样。因此省略其说明。接着对使用了随时间变化的锁的锁信息的秘密传送步骤进行说明。DVD 驱动 1500-1 使用共享了的随时间变化的锁对加密盘锁集进行总线加密，并把改动检查码授与介质 ID。然后，DVD 驱动 1500-1 把加密盘锁集和介质 ID 传送给 MPEG 解码器模块 1500-2。MPEG 解码器模块 1500-2 使用共享了的随时间变化的锁对接收到的被进行总线加密了的加密盘锁集进行总线解码。还有，在 MPEG 解码器模块 1500-2 中，使用共享了的随时间变化的锁对被授予介质 ID 的改动检查码进行检查。

最后对被扰频的信息信号（内容）的解码进行说明。MPEG 解码器模块 1500-2 从 DVD-R 盘 1550 的用户区读出加密标题锁和被扰频的信息信号（AV 数据）。然后，MPEG 解码器模块 1500-2 用被解码了的加密盘锁集对盘锁进行解码，并用该盘锁对盘固有锁进行解码。还有，用该盘固有锁对标题锁进行解码，并用该标题锁对被扰频的信息信号进行去扰频。

如上所述，被扰频的信息信号的解码所必需的锁等信息对再生型 DVD（DVD-ROM 盘）和记录型 DVD（DVD-R 盘）不同，因此被传输的数据和传输步骤不同。本发明用 DVD 驱动部识别存储盘类别并依照与此对应的传输步骤进行控制。在 MPEG 解码器模块中，从数据传输步骤的

不同识别存储盘类别， 并通过与被叠加在电子水印信息上的存储盘类别进行一致性比较可以进行再生限制。还有，在图 14 和图 15 中，在再生型 DVD 和记录型 DVD 上使用相同的认证方法。但是，通过在再生型 DVD 和记录型 DVD 上使用不同的认证方法，MPEG 解码器模块可以从认证方法的不同与上述的情形一样地识别存储盘类别。作为不同的认证方法有使用不同算法（上述函数 f）的认证方法、以及即使是相同的算法也在算法中使用不同的参数等的认证方法。

在到目前为止的说明中，通过扰频对信息信号进行了加密，但如果用其他的方式进行加密也可以得到同样的效果。

在本实施例中，对把光盘用作信息记录介质的情形进行了说明。但是，该说明对于其他的半导体存储器和磁记录介质（硬盘等）也可以以同样的方法适用。还有，本发明的被加密了的信息信号也可以通过因特网等网络线路（传送介质）被传送。此时，通过依照上述认证步骤在接收方和发送方进行认证可以防止非法复制。

如上所述，根据本发明，对成为规定的复制控制对象的信息信号（例如，禁止除此以外的复制或绝对禁止复制的信息信号），把表示该信息信号被扰频的扰频信息作为电子水印信息叠加，而且，根据信息记录介质的类别进行相应的扰频并往信息记录介质进行记录。由此，在解读了扰频后可以限制往信息记录介质的非法记录和从非法复制的其他种类的信息记录介质的再生。对后者更具体地说，信息再生装置对表示被叠加在读出的信息信号上的电子水印信息（扰频信息）的状态和读出的信息信号的扰频状态（是否被扰频）进行比较。由此，当比较结果不一致时，可以防止从通过非法复制制成的信息记录介质进行的再生。还有，根据本发明，在信息再生装置中，不进行电子水印信息的改写，因此，不需要安装电子水印信息的改写部，可以取低价的构成。

说 明 书 附 图

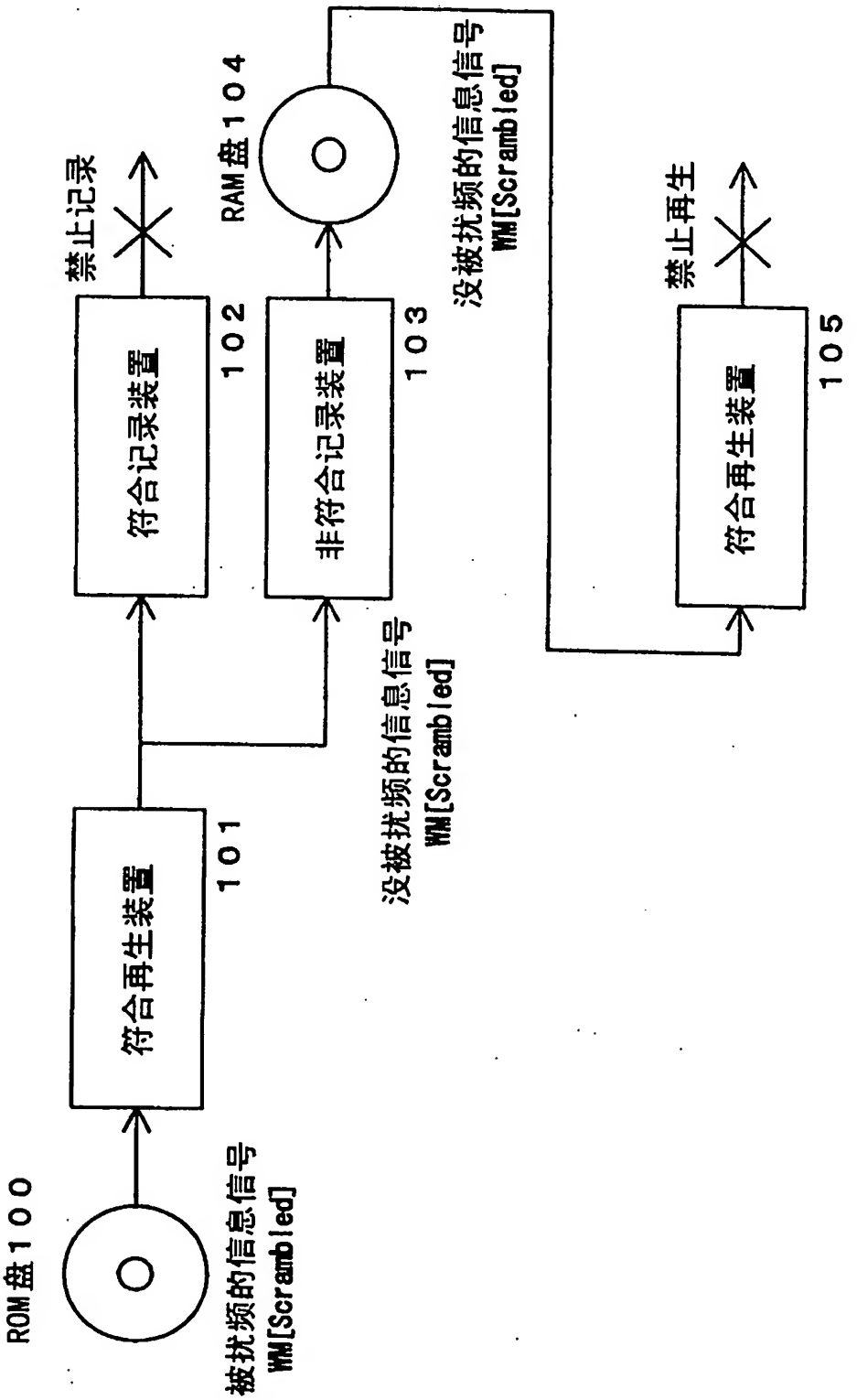
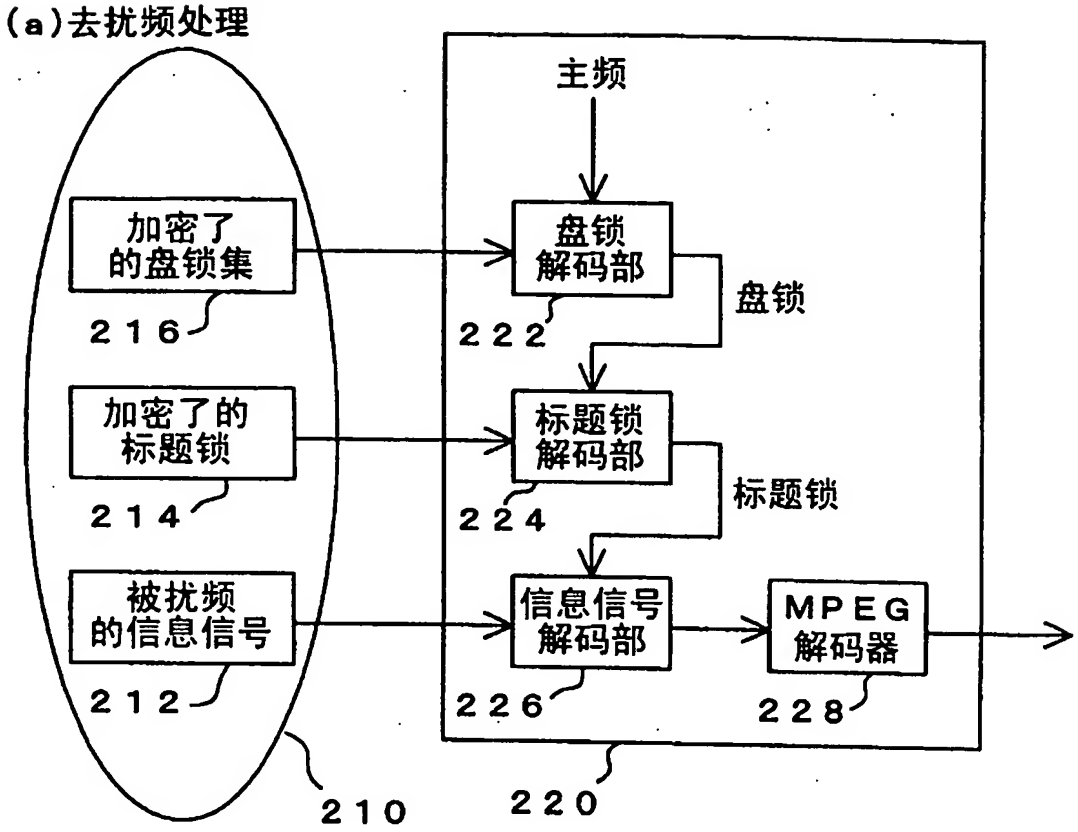

ROM盘100
被扰频的信息信号
WM[Scrambled]
符合再生装置
101
符合记录装置
102
禁止记录
非符合记录装置
103
RAM盘104
没被扰频的信息信号
WM[Scrambled]
没被扰频的信息信号
WM[Scrambled]
符合再生装置
105
禁止再生

图 1


(a)去扰频处理
主频
加密了的盘锁集
216
盘锁解码部
222
盘锁
加密了的标题锁
214
标题锁解码部
224
标题锁
被扰频的信息信号
212
信息信号解码部
226
MPEG解码器
228
210
220

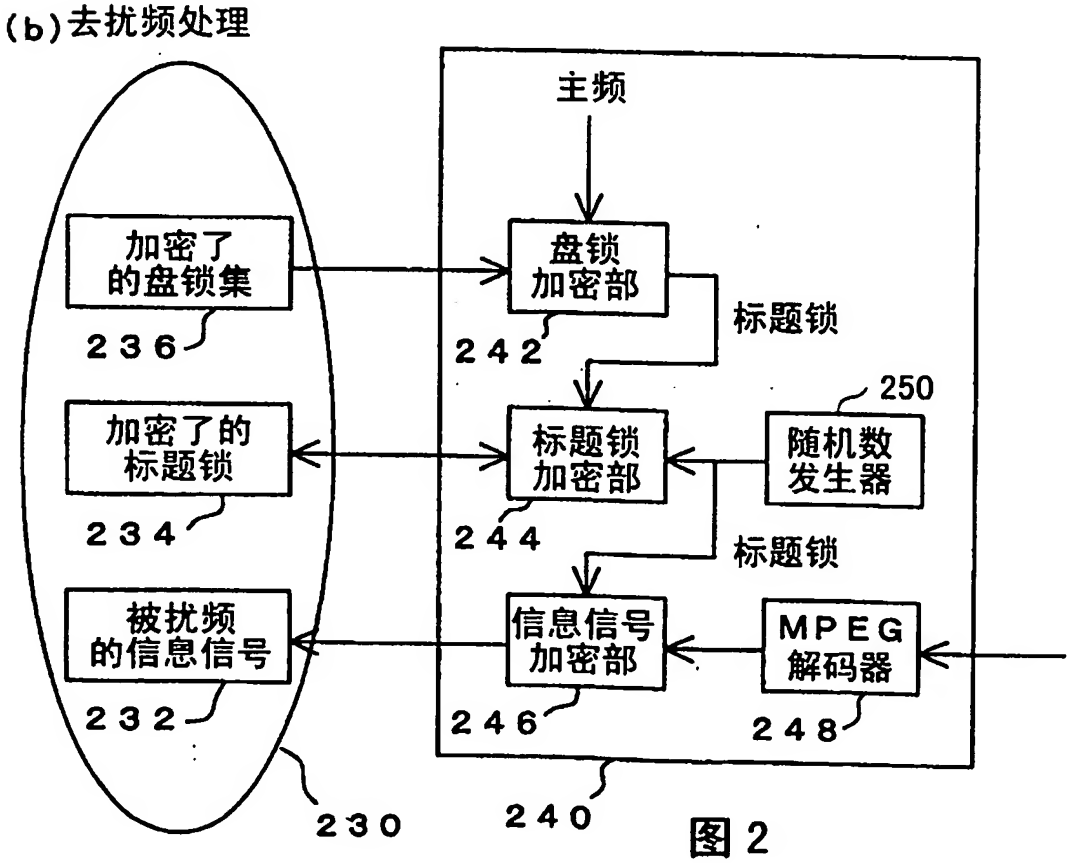

(b)去扰频处理
主频
加密了的盘锁集
236
盘锁加密部
242
标题锁
250
加密了的标题锁
234
标题锁加密部
244
随机数发生器
标题锁
被扰频的信息信号
232
信息信号加密部
246
MPEG解码器
248
230
240

图 2

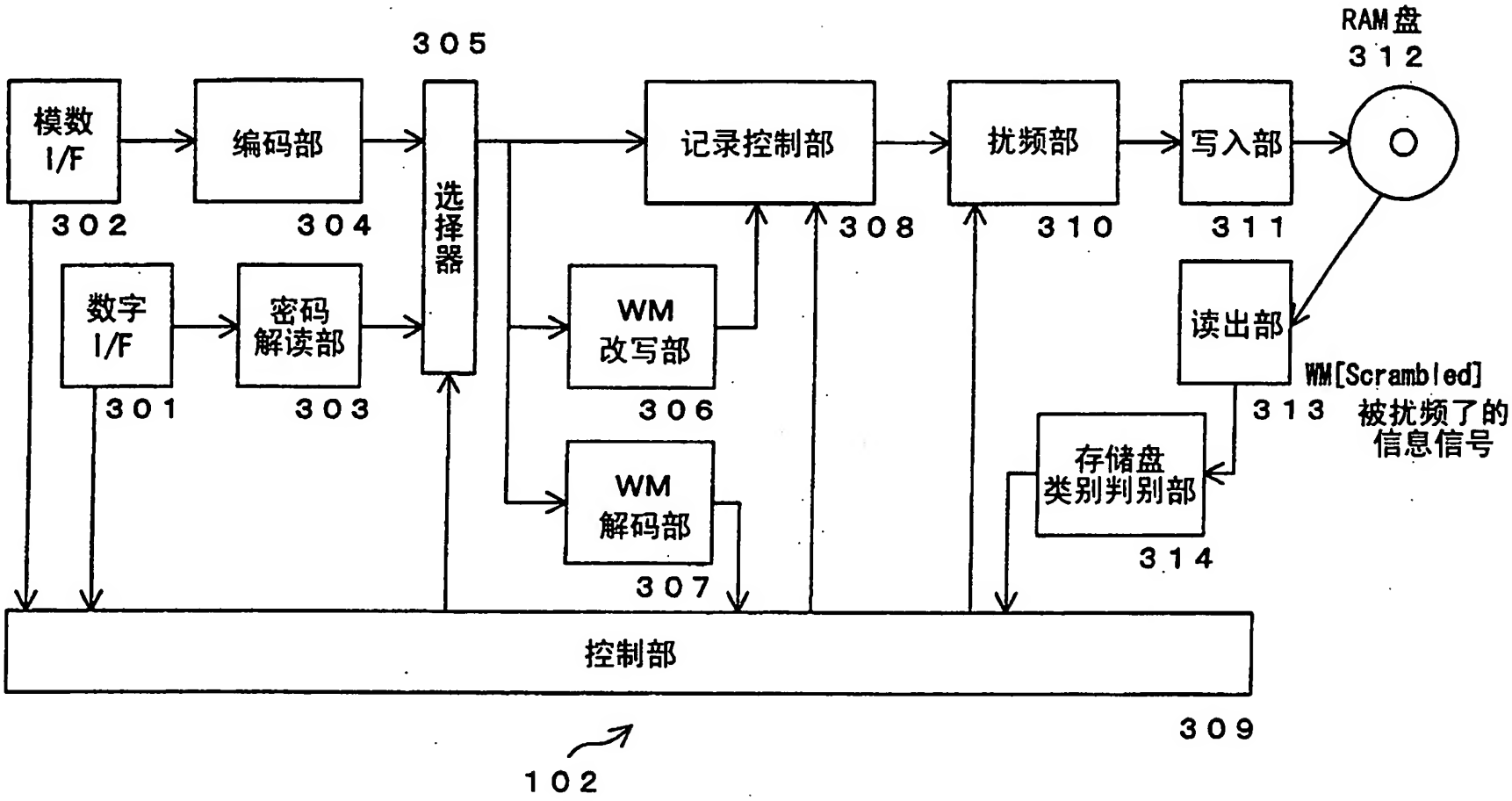

RAM盘
312
305
模数
I/F
302
编码部
304
选择器
记录控制部
308
扰频部
310
写入部
311
数字
I/F
301
密码
解读部
303
WM
改写部
306
读出部
313
WM[Scrambled]
被扰频了的
信息信号
WM
解码部
307
存储盘
类别判别部
314
控制部
309
102

图 3

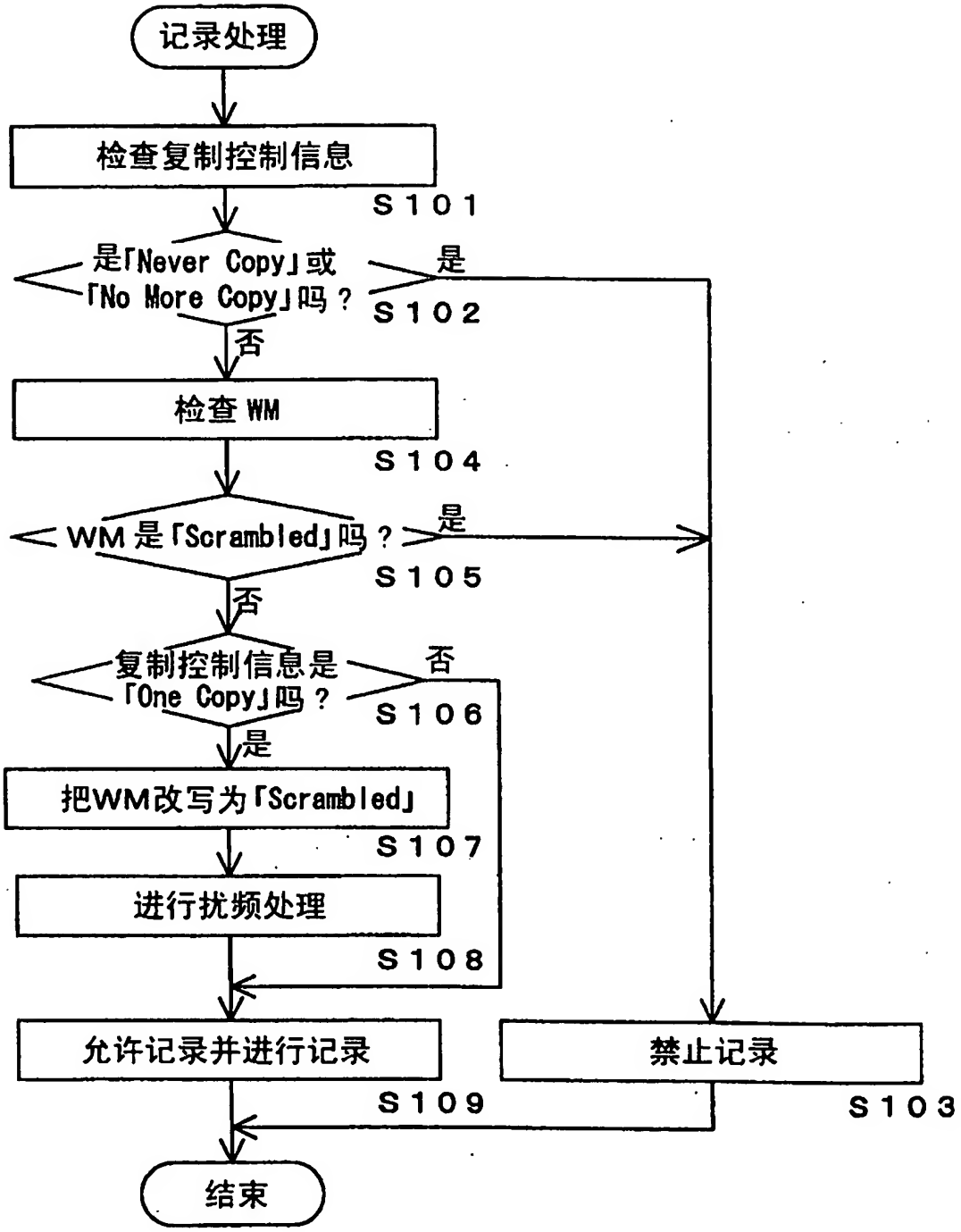

记录处理
检查复制控制信息
S101
是「Never Copy」或「No More Copy」吗？
是
S102
否
检查 WM
S104
WM 是「Scrambled」吗？
是
S105
否
复制控制信息是「One Copy」吗？
否
S106
是
把WM改写为「Scrambled」
S107
进行扰频处理
S108
允许记录并进行记录
S109
禁止记录
S103
结束

图 4

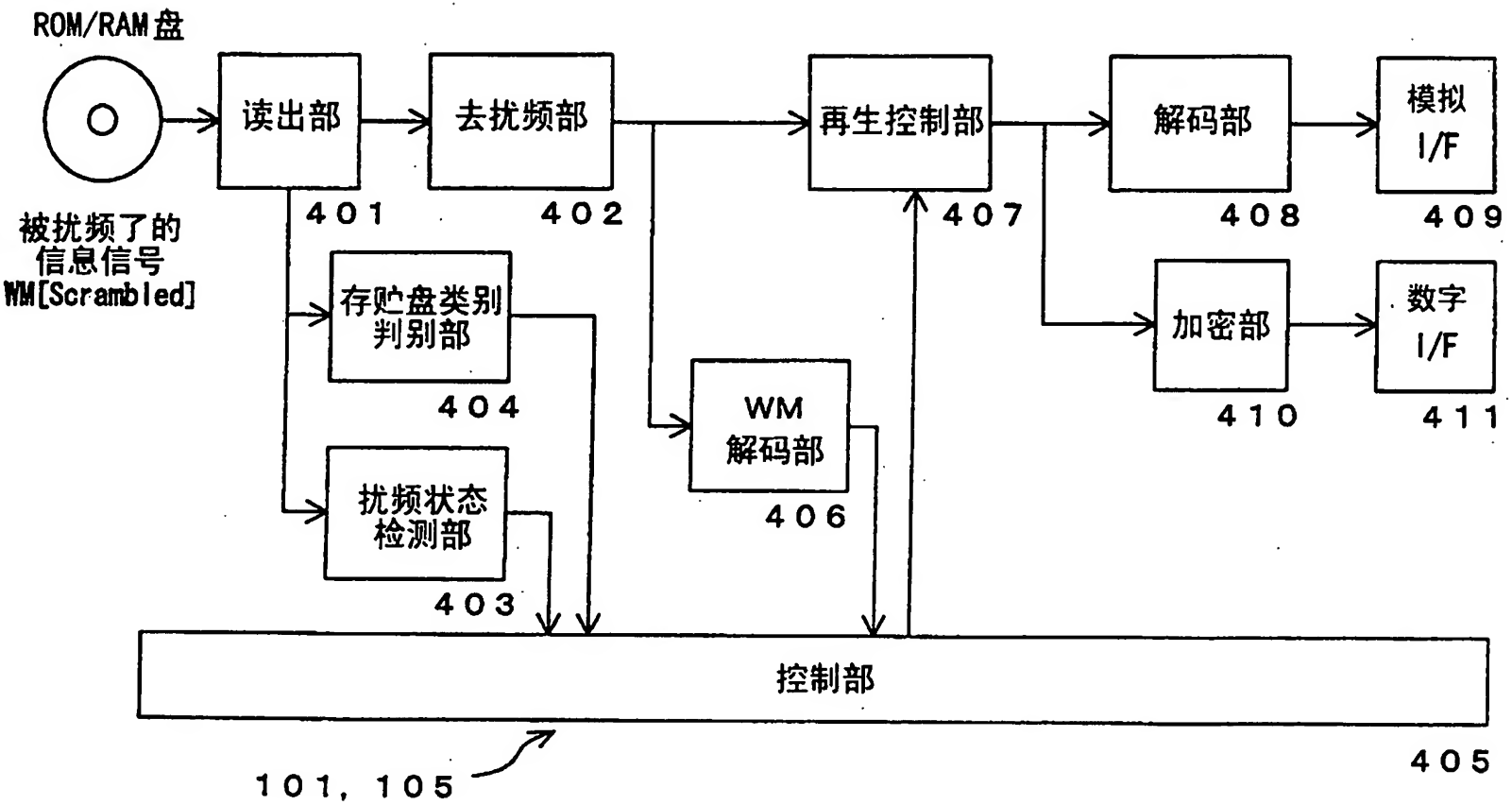

ROM/RAM盘
被扰频了的
信息信号
WM[Scrambled]
读出部
401
去扰频部
402
再生控制部
407
解码部
408
模拟
I/F
409
存贮盘类别
判别部
404
加密部
410
数字
I/F
411
WM
解码部
406
扰频状态
检测部
403
控制部
405
101，105

图 5

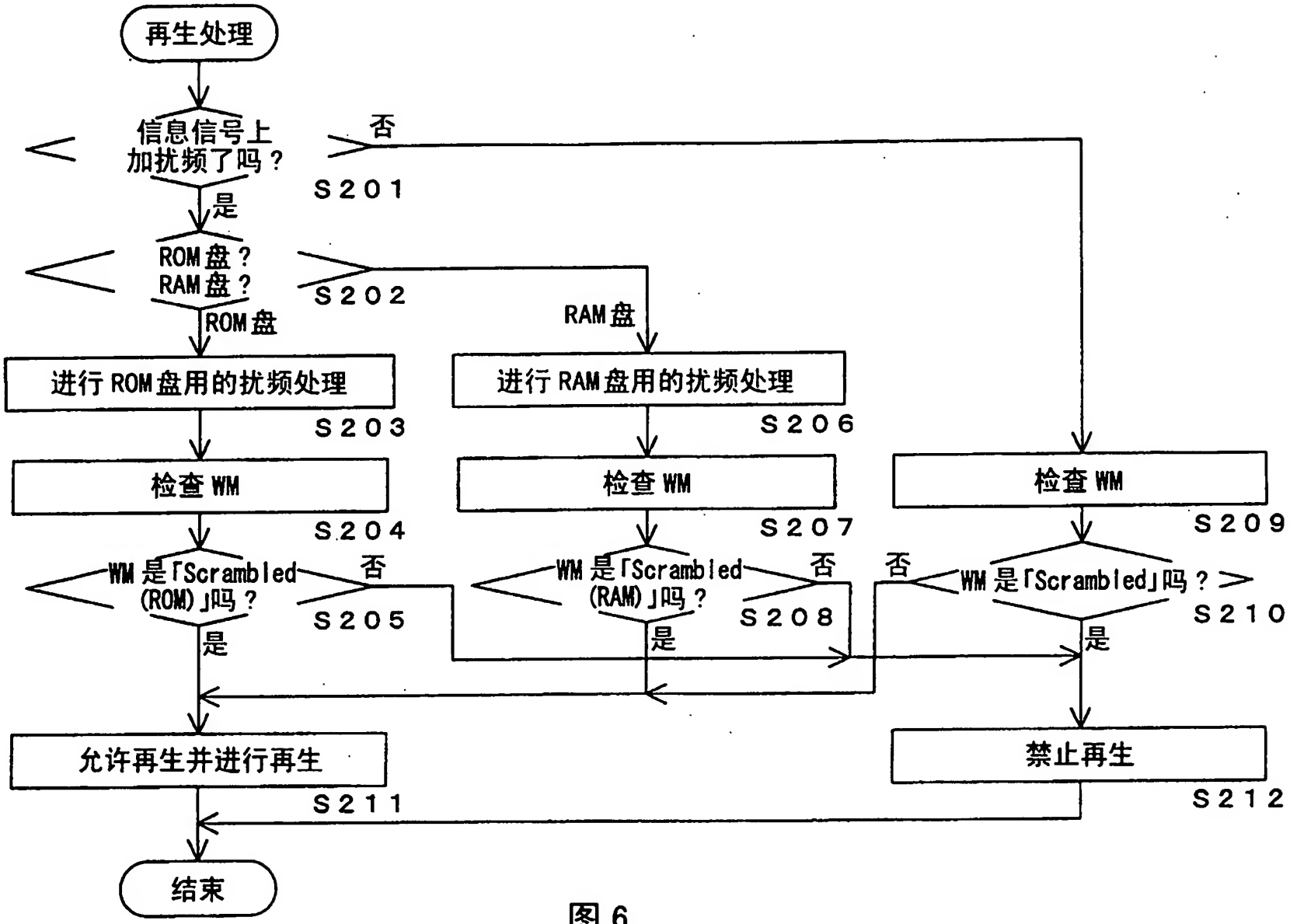

再生处理
信息信号上加扰频了吗？
否
S201
是
ROM盘？RAM盘？
S202
ROM盘
RAM盘
进行ROM盘用的扰频处理
S203
进行RAM盘用的扰频处理
S206
检查WM
S204
检查WM
S207
检查WM
S209
WM是「Scrambled(ROM)」吗？
否
S205
WM是「Scrambled(RAM)」吗？
否
S208
否
WM是「Scrambled」吗？
S210
是
是
是
允许再生并进行再生
S211
禁止再生
S212
结束

图 6

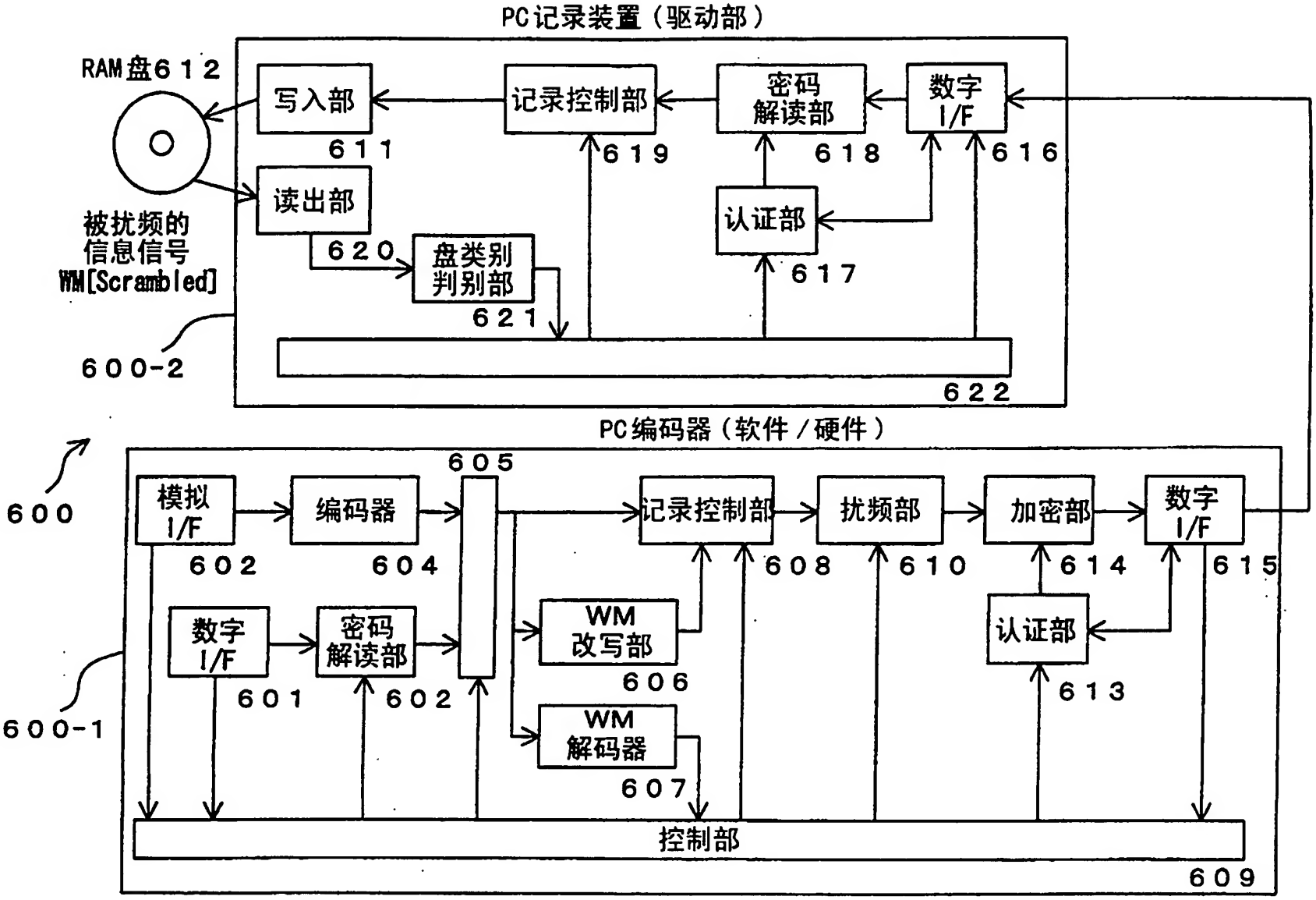

PC记录装置（驱动部）
RAM盘612
写入部
611
记录控制部
619
密码
解读部
618
数字
I/F
616
读出部
620
盘类别
判别部
621
认证部
617
被扰频的
信息信号
WM[Scrambled]
600-2
622
PC编码器（软件／硬件）
600
605
模拟
I/F
602
编码器
604
记录控制部
608
扰频部
610
加密部
614
数字
I/F
615
数字
I/F
601
密码
解读部
602
WM
改写部
606
认证部
613
600-1
WM
解码器
607
控制部
609

图 7

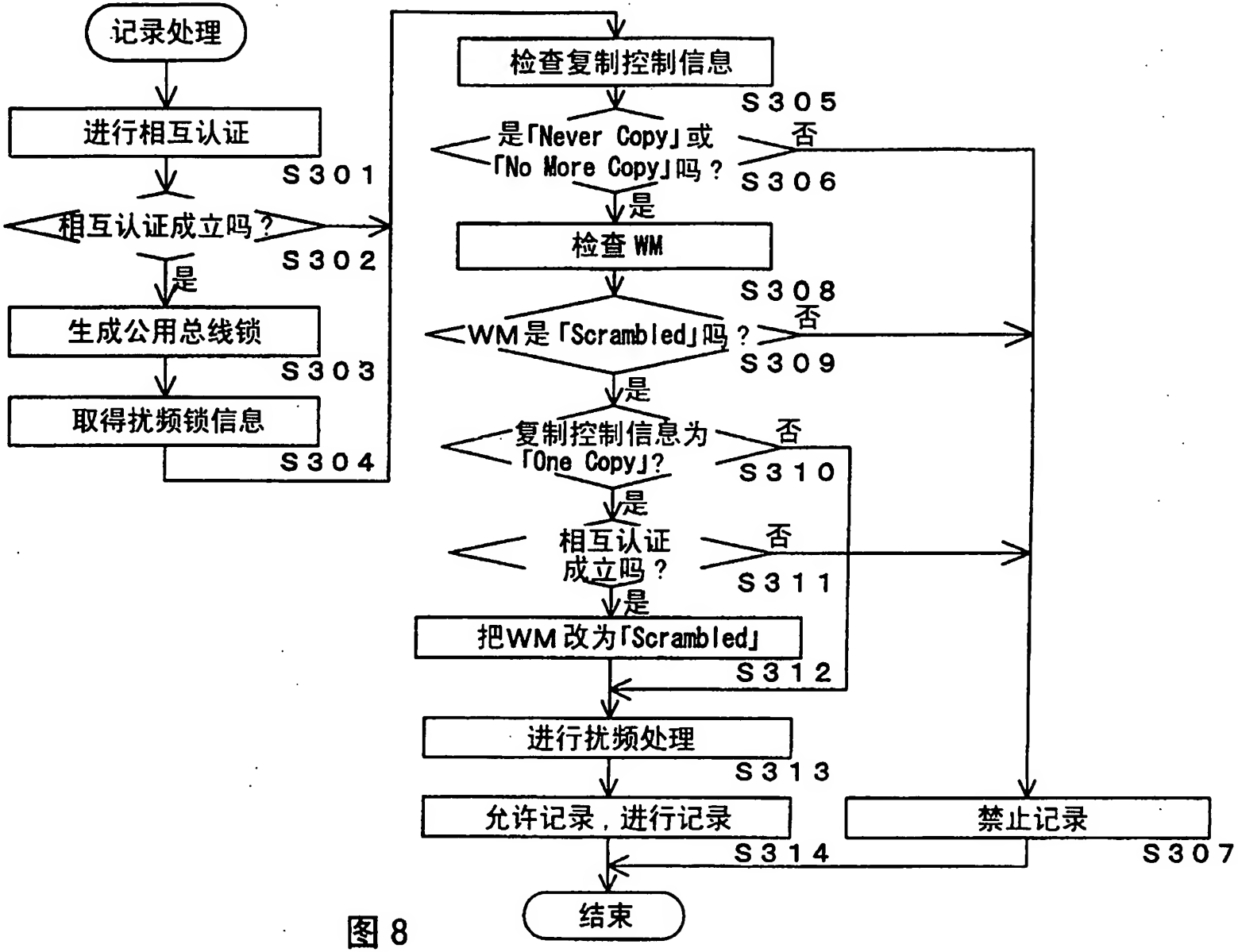

记录处理
进行相互认证
S301
相互认证成立吗？
S302
否
是
生成公用总线锁
S303
取得扰频锁信息
S304
检查复制控制信息
S305
是「Never Copy」或「No More Copy」吗？
S306
否
是
检查 WM
S308
WM是「Scrambled」吗？
S309
否
是
复制控制信息为「One Copy」?
S310
否
是
相互认证成立吗？
S311
否
是
把WM改为「Scrambled」
S312
进行扰频处理
S313
允许记录，进行记录
S314
禁止记录
S307
结束

图 8

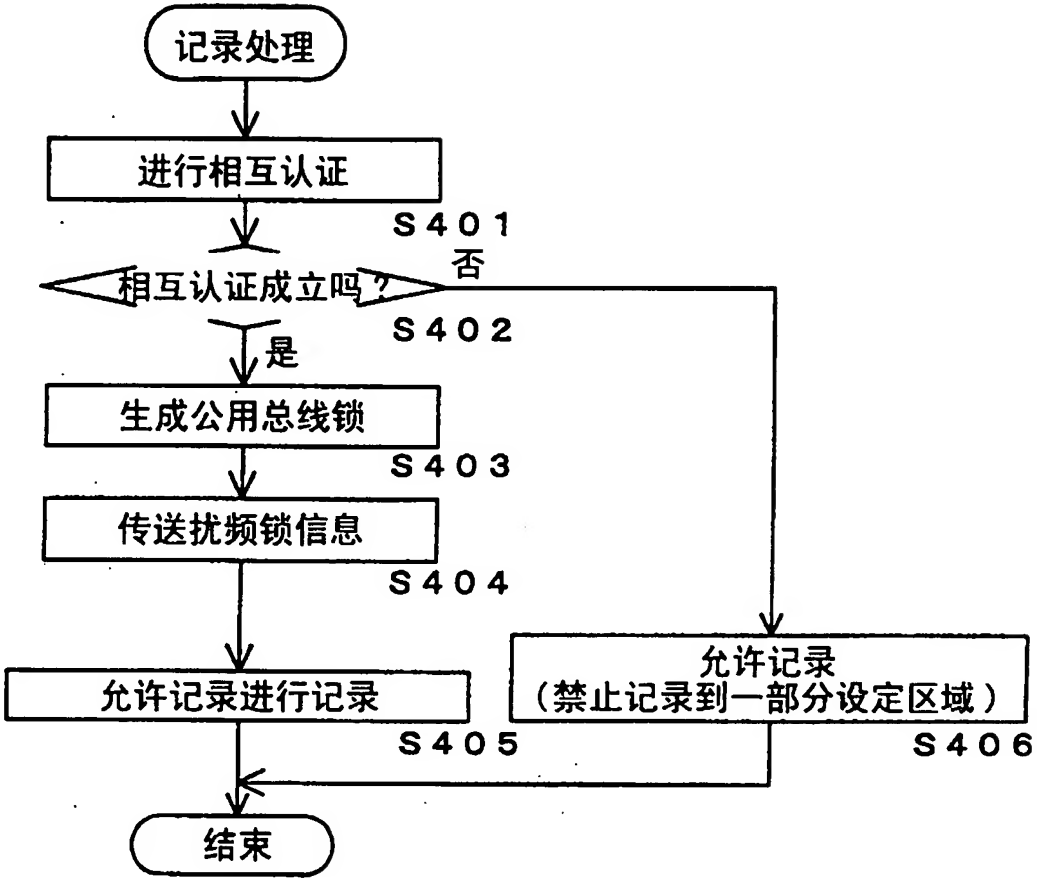

记录处理
进行相互认证
S401
相互认证成立吗？
否
S402
是
生成公用总线锁
S403
传送扰频锁信息
S404
允许记录进行记录
S405
允许记录
（禁止记录到一部分设定区域）
S406
结束

图 9

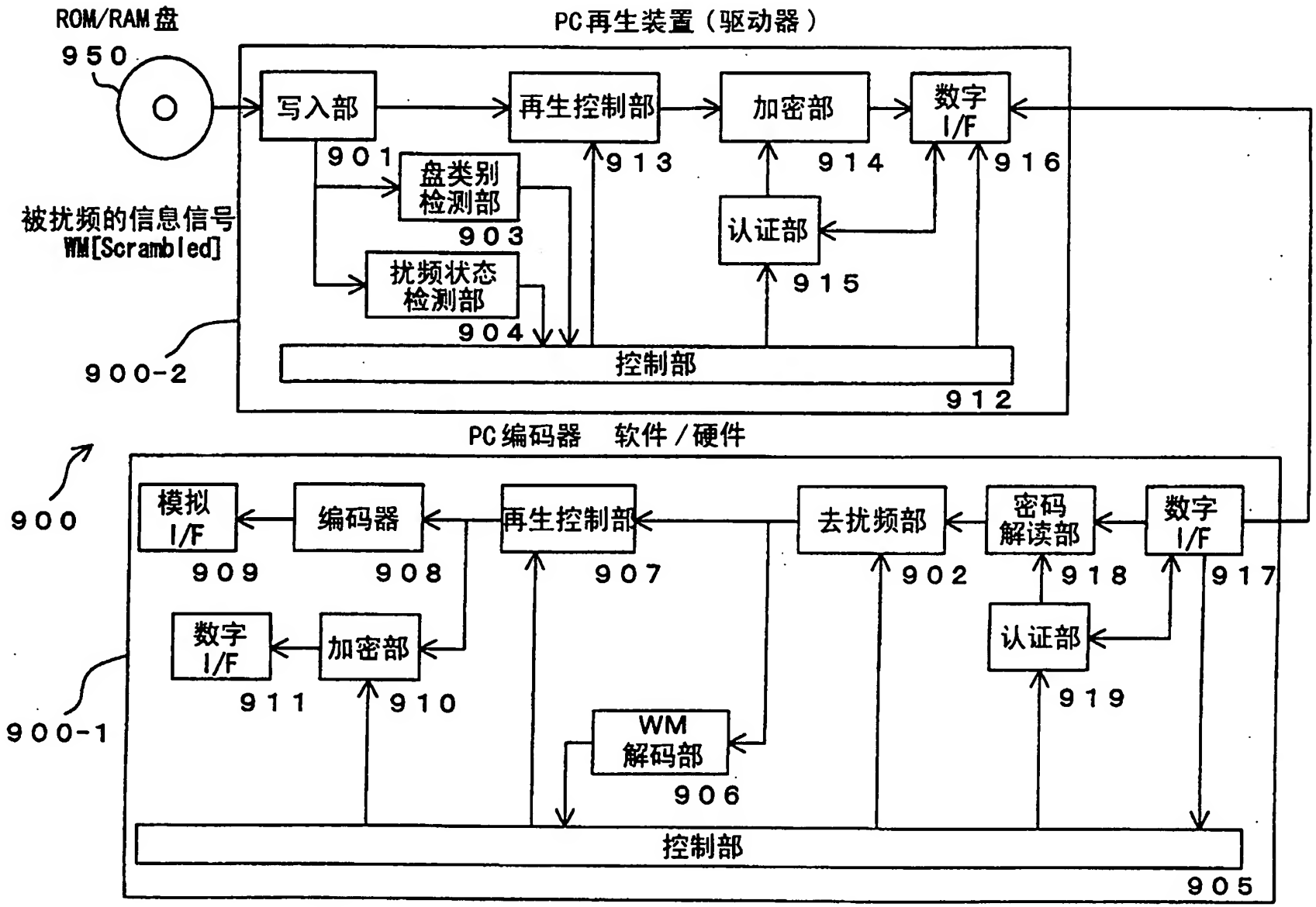

ROM/RAM盘
950
PC再生装置（驱动器）
写入部
901
再生控制部
913
加密部
914
数字
I/F
916
盘类别
检测部
903
被扰频的信息信号
WM[Scrambled]
扰频状态
检测部
904
认证部
915
900-2
控制部
912
PC编码器　软件／硬件
900
模拟
I/F
909
编码器
908
再生控制部
907
去扰频部
902
密码
解读部
918
数字
I/F
917
数字
I/F
911
加密部
910
认证部
919
900-1
WM
解码部
906
控制部
905

图 10

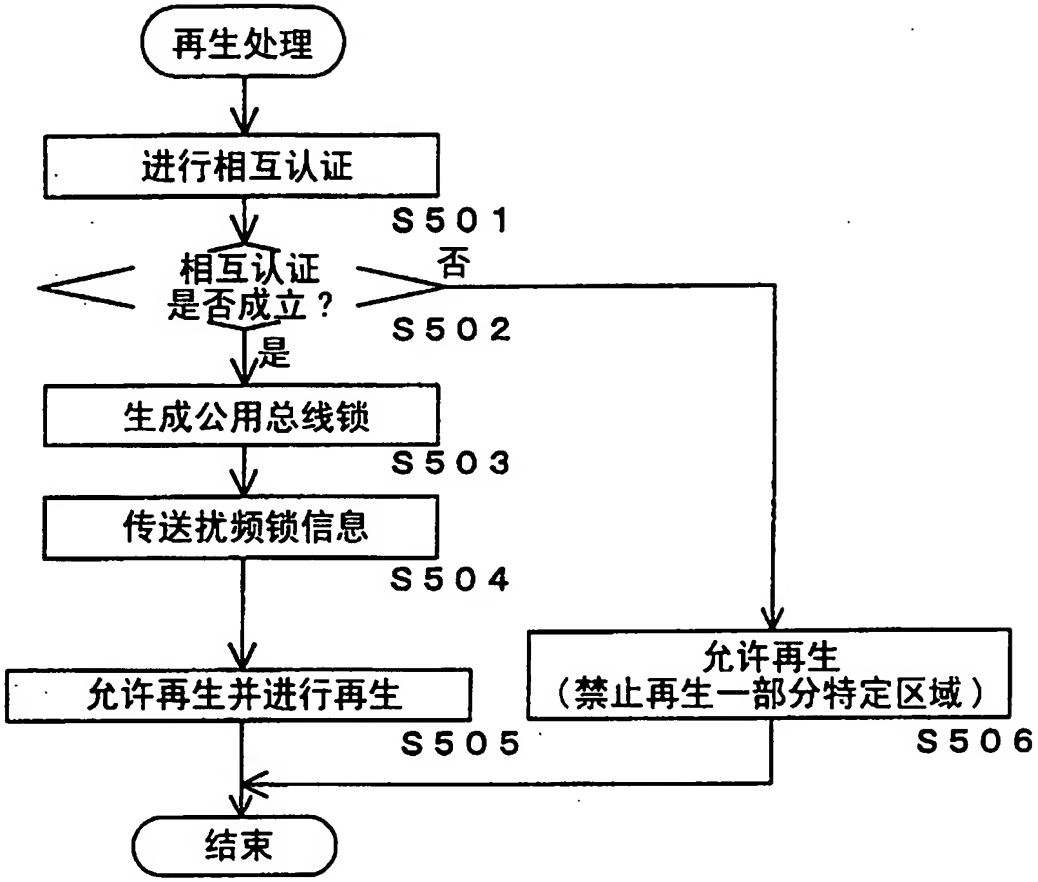

再生处理
进行相互认证
S501
相互认证
是否成立？
否
S502
是
生成公用总线锁
S503
传送扰频锁信息
S504
允许再生并进行再生
S505
允许再生
（禁止再生一部分特定区域）
S506
结束

图 11

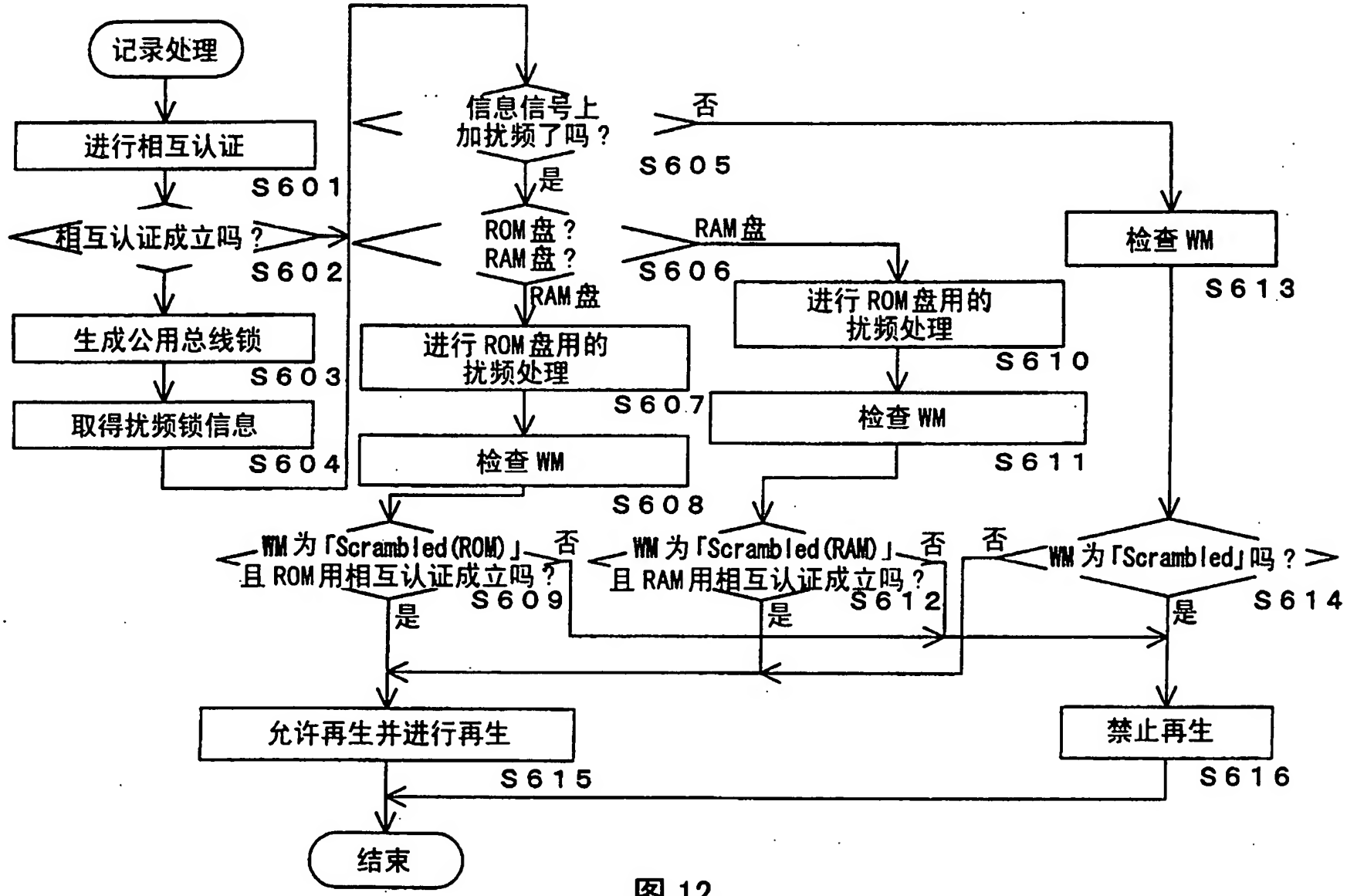

记录处理
进行相互认证
S601
相互认证成立吗？
S602
生成公用总线锁
S603
取得扰频锁信息
S604
信息信号上加扰频了吗？
否
S605
是
ROM盘？
RAM盘？
RAM盘
S606
RAM盘
进行ROM盘用的扰频处理
S607
检查WM
S608
WM为「Scrambled(ROM)」且ROM用相互认证成立吗？
否
S609
是
进行ROM盘用的扰频处理
S610
检查WM
S611
WM为「Scrambled(RAM)」且RAM用相互认证成立吗？
否
S612
是
检查WM
S613
否
WM为「Scrambled」吗？
S614
是
允许再生并进行再生
S615
禁止再生
S616
结束

图 12

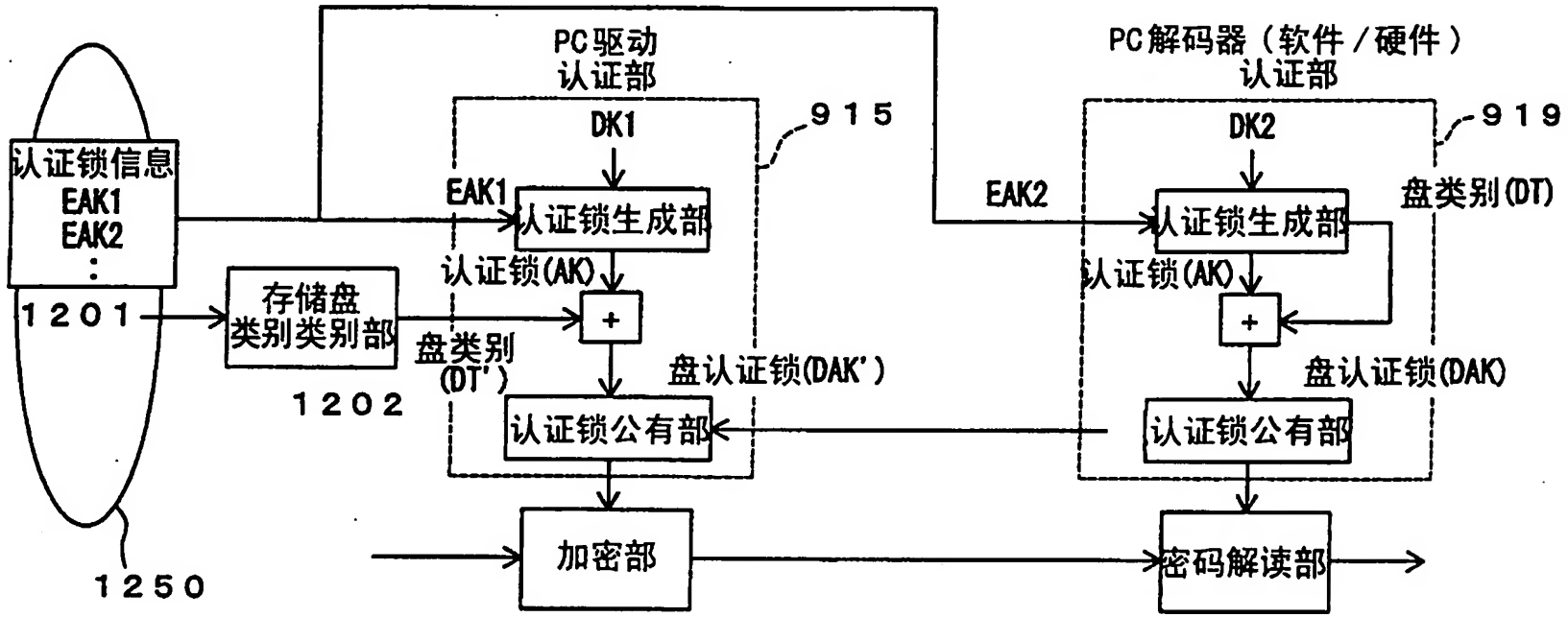

PC驱动
认证部
915
DK1
EAK1
认证锁生成部
认证锁(AK)
+
盘认证锁(DAK')
认证锁公有部
PC解码器（软件／硬件）
认证部
919
DK2
EAK2
盘类别(DT)
认证锁生成部
认证锁(AK)
+
盘认证锁(DAK)
认证锁公有部
认证锁信息
EAK1
EAK2
:
1201
存储盘
类别类别部
1202
盘类别
(DT')
1250
加密部
密码解读部

图 13

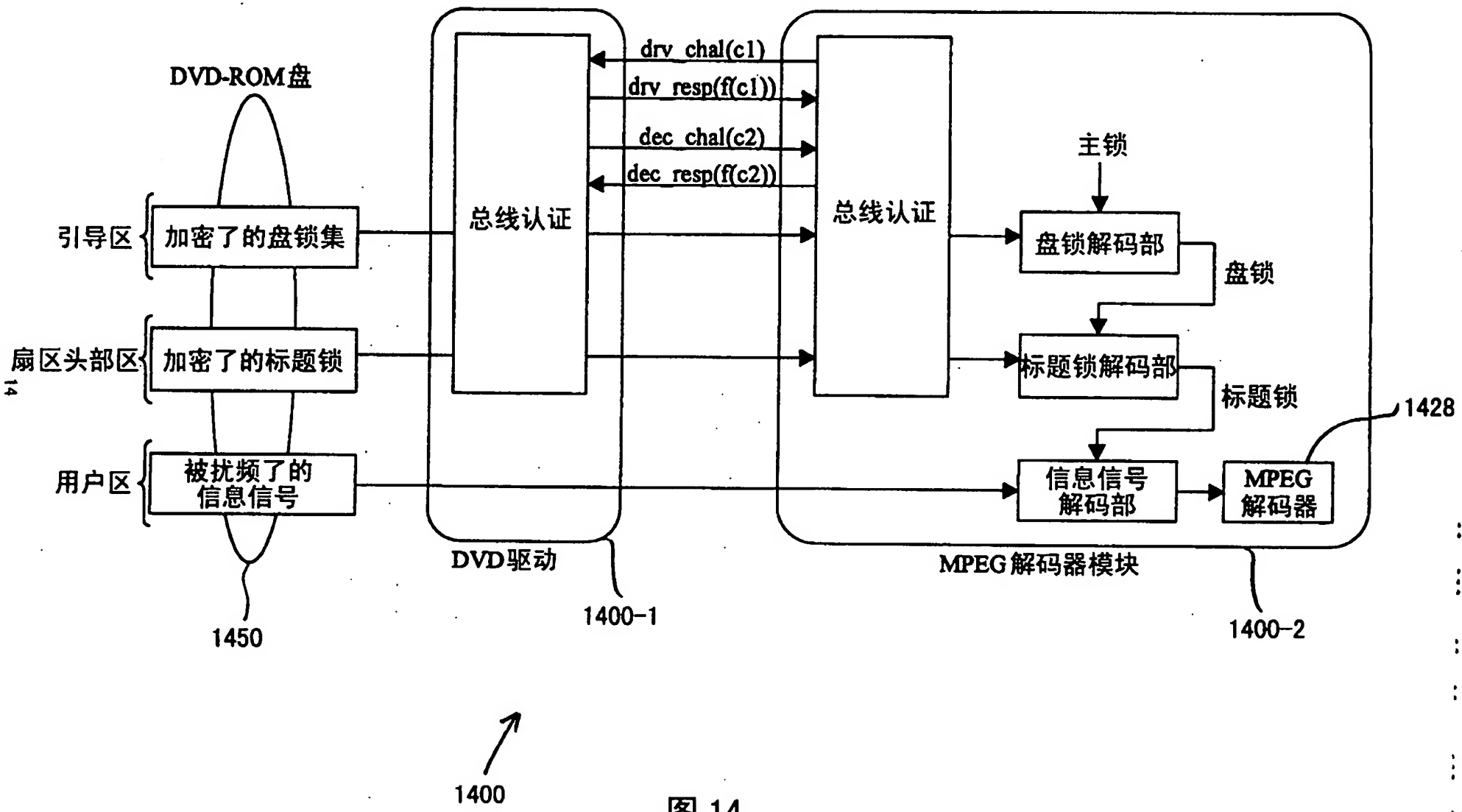

DVD-ROM盘
引导区
加密了的盘锁集
扇区头部区
加密了的标题锁
用户区
被扰频了的
信息信号
1450
总线认证
DVD驱动
1400-1
drv_chal(c1)
drv_resp(f(c1))
dec_chal(c2)
dec_resp(f(c2))
总线认证
主锁
盘锁解码部
盘锁
标题锁解码部
标题锁
信息信号
解码部
MPEG
解码器
1428
MPEG解码器模块
1400-2
1400

图 14

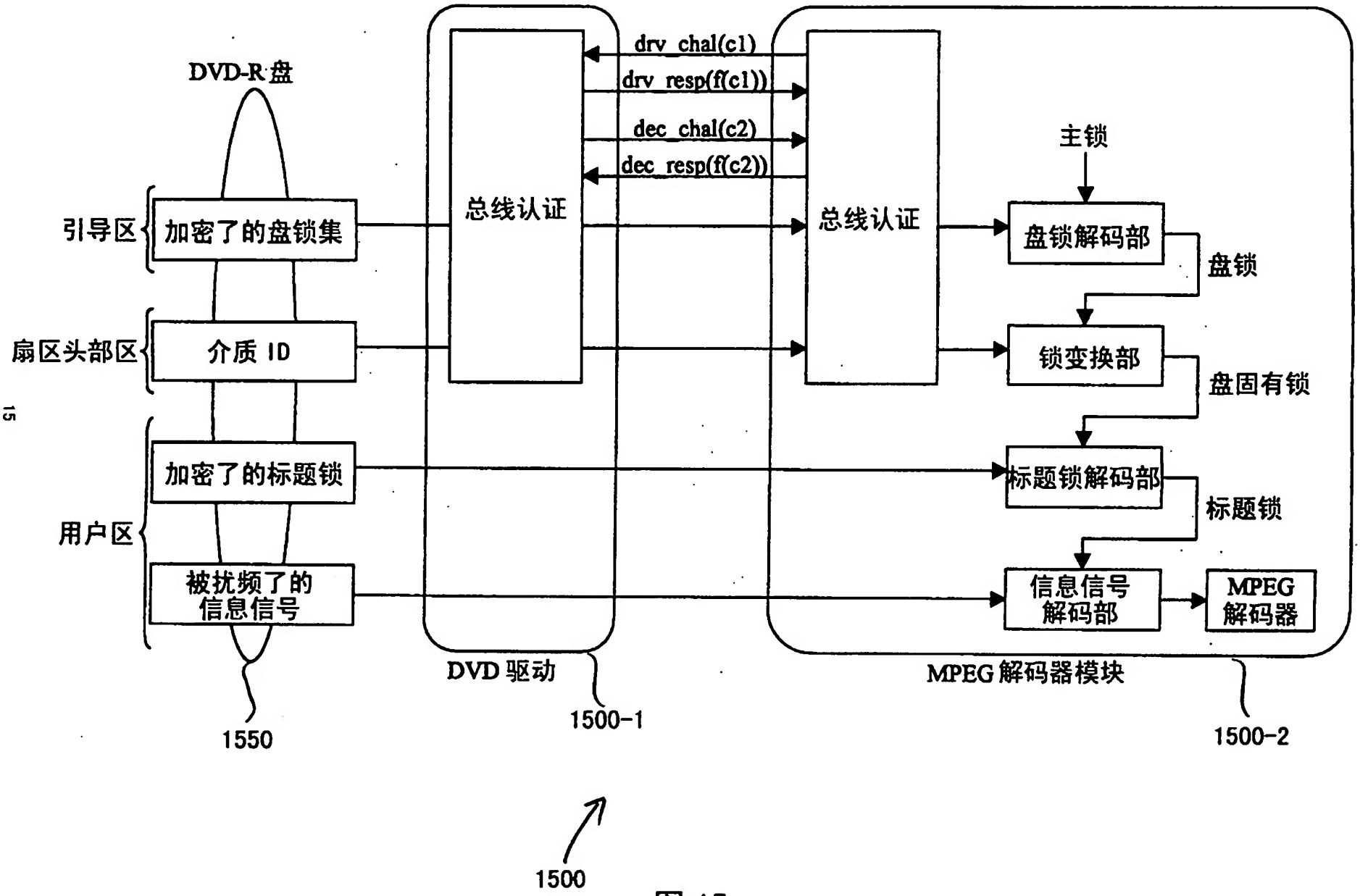

DVD-R 盘
引导区
加密了的盘锁集
扇区头部区
介质 ID
用户区
加密了的标题锁
被扰频了的
信息信号
1550
总线认证
DVD 驱动
1500-1
drv_chal(c1)
drv_resp(f(c1))
dec_chal(c2)
dec_resp(f(c2))
总线认证
主锁
盘锁解码部
盘锁
锁变换部
盘固有锁
标题锁解码部
标题锁
信息信号
解码部
MPEG
解码器
MPEG 解码器模块
1500-2
1500

图 15

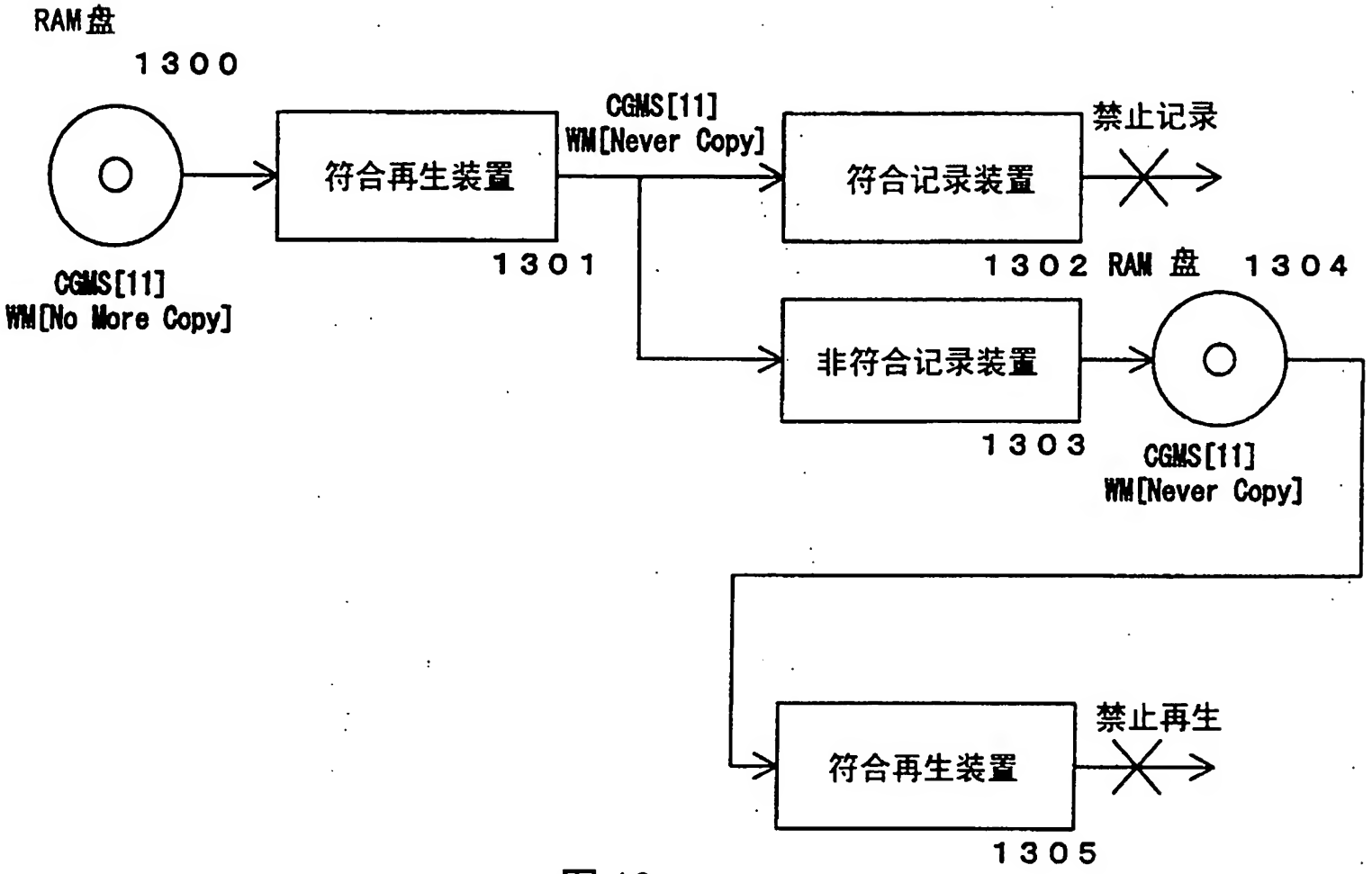

RAM盘
1300
CGMS[11]
WM[No More Copy]
符合再生装置
1301
CGMS[11]
WM[Never Copy]
符合记录装置
禁止记录
1302
RAM 盘
1304
非符合记录装置
1303
CGMS[11]
WM[Never Copy]
符合再生装置
禁止再生
1305

图 16